PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-258838

(43)Date of publication of application : 12.09.2003

(51)Int.Cl. H04L 12/56

H04L 12/66

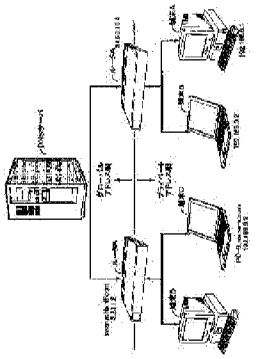
(21)Application number : 2002-058260

(22)Date of filing : 05.03.2002

(71)Applicant : FUJITSU LTD

(72)Inventor : OGAWA ATSUSHI

(54) COMMUNICATION EQUIPMENT AND NETWORK SYSTEM



(57)Abstract:

PROBLEM TO BE SOLVED: To access a private address network from a global address network.

SOLUTION: An address conversion device manages respective nodes (terminals A to D) by attaching a unique name (PC-B. home-a. com as a FQDN (fully qualified domain name)) to the respective nodes belonging to a private address network, and acquires a corresponding private address (192.168.0.2, for

example, when query is made about PC-B.home-a.com) and notifies, when a prescribed name is inquired from a global address network or a prescribed node belonging to another private address network. A DNS (domain name system) server within the global address network which does not belong to a tree of a DNS server within global address network is prepared for each private address network, and the problem of the name of a private address can be solved via the global address network by making the DNS server accessible from the global address network.

LEGAL STATUS

[Date of request for examination]	24.02.2005
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the communication device which has the 2nd network which consists of terminals which belong to the 1st network which consists of communication devices which have the address of the 1st type, and have the address of the 2nd type in the subordinate the identifier the terminal belonging to the network of the subordinate of other communication devices was named -- being concerned -- others -- with a means to manage corresponding to the identifier the communication device was named The communication device characterized by establishing a means to output the demand of address solution to the communication device which corresponds with said management tool when the identifier the terminal used as a communications partner was named from a subordinate's terminal is received.
[Claim 2] a means to make the address of the subordinate's terminal correspond with the identifier to which it was attached by the terminal, and to manage it -- said -- others -- the demand of the address solution of the terminal of the subordinate from a communication device -- receiving -- said management tool -- the address -- solving -- said -- others -- the communication device according to claim 1 characterized by establishing a means to notify the address solved to the communication device.
[Claim 3] The communication device according to claim 2 characterized by to establish a means matches the address which received the notice with the dummy address which is said 2nd type of address and changed into the address which is not used as the address of the terminal the subordinate's network, and

manage when the notice of solution of the address is received from a communication device besides the above to the demand of address solution, and a means notify said address after conversion to the terminal which required a communication link.

[Claim 4] The communication device according to claim 3 characterized by establishing a means to change a dummy address into the address of a communication device besides the above when a packet with the dummy address after a notice is received from the terminal which required the communication link.

[Claim 5] In the network system which consists of the 1st network which consists of communication devices which have the address of the 1st type, and the 2nd network which consists of terminals which have the address of the 2nd type under the command of a communication device The 1st management tool which the address of the subordinate's terminal is made to correspond to said communication device with the identifier to which it was attached by each terminal, and is managed, The 2nd management tool which the identifier of a terminal is made to correspond with the communication device which manages the address of the terminal, and manages it, The network system characterized by asking for other communication devices which solve the address of the terminal of a communications partner to ****** and the communication link demand from a subordinate's terminal with said 2nd management tool, and performing address solution with said 1st management tool with other communication devices.

[Claim 6] The global address network with which each node has the unique address, and the private address network which has the address which is not unique, In the network system which has address translation equipment which changes the address in case data are transmitted among these said address translation equipment A unique identifier is given and managed to each node belonging to said private address network. The network system characterized by what a corresponding private address is acquired and notified for when the

inquiry to a predetermined identifier is made from the predetermined node belonging to said global address network or other private address networks.
[Claim 7] The global address network with which each node has the unique address, and the private address network which has the address which is not unique, The 1st address translation equipment which performs address translation in said global address network, In the network system which has the 2nd address translation equipment which performs address translation between said global address networks and said private address networks Said 1st and 2nd address translation equipment by establishing a connection independently, respectively and exchanging the information about a connection mutually between said global address network and said private network network The network system characterized by what transfer of data is enabled for.
[Claim 8] Said 1st address translation equipment is a network system according to claim 7 characterized by notifying the information about said connection to said 2nd address translation equipment in case a transmit terminal establishes a connection.
[Claim 9] For the actual private address of an accepting station, said 1st address translation equipment is a network system according to claim 8 characterized by notifying the address of a different dummy to a transmit terminal.
[Claim 10] For the actual private address of said accepting station, the address of said dummy is a network system according to claim 9 characterized by being the address with which network classes differ.

[Translation done.]

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the communication device and network system which have the global address network with which each node has the unique address especially, the private address network which has the address which is not unique, and address translation equipment which changes the address in case data are transmitted among these about a communication device and a network system.

[0002]

[Description of the Prior Art] The IP address used for the Internet communication link is managed internationally, and when performing the Internet communication link, distribution of the IP address (although called a formula IP address, it is hereafter described as a global IP address) which becomes unique in the Internet, or a domain name is to be received from the management engine (provider who is approved as Japan Network Information Center JPNIC or its proxy in the case of Japan) which received request from the international engine or it which has managed the IP address unitary. Therefore, if a global IP address is not acquired, the Internet communication link cannot be performed, and it is to communicate.

[0003] On the other hand, in networks, such as LAN (Local Area Network) which does not perform the Internet communication link, the IP address (IP addresses other than a global IP address are hereafter described as a private IP address) of arbitration can be used. However, it sets to RFC (Request For Comments) which IETF (International Engineering Task Force) which is the standardization organization of the Internet technique exhibits. So that a problem may not arise, when the terminal which is using the private IP address is wrong and an Internet

connectivity is performed In LAN which does not perform an Internet connectivity, using an IP address (it being hereafter described as a private IP address, although it is a kind of the private address) with the specific number which that it is not a global IP address can identify is recommended (it mentions later for details).

[0004] On the other hand, since it is the situation that we are anxious about an exhaustion of a global IP address, with the rapid increment in the Internet communication link in recent years, the situation which a global IP address cannot fully distribute to networks which need a lot of IP addresses, such as a company and a self-governing body, has arisen. In order to cope with lack of such a global IP address, when using a private IP address (or private IP address) inside LAN and performing the Internet communication link with an external network in a company etc., the method of using a global IP address is becoming general.

[0005] However, the cases where he wants to connect LAN built using the private IP address only supposing connection within LAN with other networks similarly built using the private IP address with the spread of the rapid increment in LAN (private network) and the Internet communication links are increasing in number. In this case, there are the following problems. The network number part which is a part of address is being fixed to the specific figure, and since the above-mentioned private IP address has the comparatively narrow range of the number which can be used as a private IP address, its possibility that the same private IP address is used in a different network is large. When carrying out direct continuation of the networks for which the same private IP address may be used, without minding the global Internet, it is desirable not to change the contents of a setting, such as a private IP address given to each terminal and a server which participates in the address. Implementation of the IP address inverter it enables it to connect, without changing the environment of each network where it has already worked from such a situation in both the separate networks that are using the private IP address uniquely is desired.

(1) Like configuration common knowledge of an IP address, the IP address in the Internet communication link which uses a TCP/IP protocol consists of 32 bits which consists of parts for a part for the address part for identifying a network (it is hereafter described as a network number), and the address part for identifying each host in the network (terminal) (it is hereafter described as a host number). However, since there is much what has many networks (local network) in a wide range area although there are few hosts of each network (local network) while there is a large-scale network with many internal hosts among the networks of a company, the digit count of a network number is changed by network scale and configuration. It is shown whether a "class" is a network which uses what figure for a network number.

[0006] Although drawing 21 illustrates the configuration of the IP address of each class, like illustration, 7 bits which a top bit is "0" and Class A follows are a network number (a network number is described also as NW number by a diagram including other drawings), and remaining 24 bits has a host number. The inside of the parenthesis of drawing 21 is the number of bits used for a network number and a host number. Moreover, in Class B, 2 bits of a head are a binary number, a top triplet is become to "111" with a binary number, and, as for the network number and Class C, the next 21 bits have become ["10" and the next 21 bits] a network number. In addition, illustration is omitted although there is a class D etc.

[0007] Although 24 bits can be used for a host number in Class A as shown in drawing 21 , it is rare to assign a host number to the terminal in a network optionally in fact, and it is common to hierarchize the inside of a network further. The part of the IP address which gave the hierarchized network to a subnetwork (it is hereafter described as a "subnet"), a call, and each subnet is called the subnet number. A subnet number uses a part of host number, and shows relation with a host number to drawing 21 . Although the number of bits of the subnet number given to the number of subnets and each subnet is optional, as for a subnet number, it is most common to assign 8 bits as a unit, as indicated to

drawing 21 .

[0008] a 32-bit IP address comes to display 8 bits of delimiters at a time with four decimal numbers as usual -- **** (each of four decimal numbers, i.e., the number of 8 bitwises, is hereafter described as a "digit") -- the numeric value of the bit which shows a class is displayed with a decimal number together with the network number in 8 bits of the beginning. According to this method of presentation, the range of the figure used for the IP address of each class becomes the value which is described in drawing 22 , and in Class A, since the first bit is "0", the first digit serves as the range of "0-127" (it is "0-126" that it can actually be used) with a decimal number (hereafter, unless it refuses, a decimal number describes especially the numeric value of each digit).

[0009] Since 2 bits of the beginning of Class B are "10" in a binary number, the numerical range of the first digit is set to "128-191." Although Class C is the same, since there are Class D (4 bits of the beginning are "1110" at a binary number) and Class E (5 bits of the beginning are "11110" at a binary number) which omitted explanation, the ranges of number which can be used for the first digit are not "192-255", and are set to "192-223." Moreover, the range of number which can be used for the network numbers or host numbers (subnet number) of triple digits other than the first digit is set to "0-255." And the IP address of each class is a decimal number as indicated on the right-hand side of drawing 22 , and it is expressed like "10. H.H.H" (example of Class A) (H is a host number and is expressed with the figure of 0-255 in fact). Therefore, the class of an IP address is discriminable with the numeric value of the first digit.

[0010] Although a global IP address or the private IP address of the configuration of the above IP address is also the same, in RFC1597 which said IETF exhibits, use of the private IP address which that it is not a global IP address can identify is recommended. Although drawing 23 shows the numeric value of the private IP address specified to RFC1597, the numerical range which can be used like illustration about the part which gave the slash about the private IP address is appointed. For example, the figure which 8 figures of the beginning are limited to

"10" (decimal number), and the private IP address of Class A uses about the first digit and the following digit in Class B and Class C is limited. Since the double figures of the beginning are limited by one numeric value, respectively in the case of Class C, there is only the 256 number of the network number which can be used for arbitration, and host numbers, respectively.

[0011] The probability for the same address to be used in a network which is different in a private IP address since the part in which the numeric value which cannot be used freely [every class] in 32 bits although it cannot say that which class is high since, as for the probability for the address completely same in a different network to be used, the number of the hosts in a network etc. influences greatly exists, and the selection range become narrow becomes high. Therefore, it needs to be premised on the same address existing in both networks when communicating in two networks which assigned the private IP address uniquely.

(2) Explain the conventional technique which connects between the terminals which carry out a group to the Internet connectivity approach of a private IP address use terminal, next two networks which are using the private IP address, respectively. With the conventional technique, when the network which is using the private IP address communicates with other networks, the approach of connecting through the global Internet is taken. Although this approach is indicated by JP,9-233112,A etc., it explains the connection method of the conventional technique to an example for the case where it is the terminal (a server is included) with which while is indicated by this official report and a terminal has a global IP address in it, hereafter.

[0012] Drawing 24 summarizes and adds the contents of explanation of this official report to the block diagram of the internetwork environment indicated by drawing 1 in said official report. Although the "formula IP address" in this official report is the same as that of the "global IP address" indicated in this specification, it is described as a formula IP address to compensate for the publication of this official report in explanation of drawing 24 . Moreover, since it is the same as that of the "private IP address" (the range is wider than the private IP address) in this

specification, a "private IP address" given [this] in an official report is used as it is.

[0013] Although only the private IP address is now given to the terminal 225 (it is described as Terminal A etc. when pointing out each terminal) in the private network 202 of drawing 24 by each, the terminal A in it shall connect to the server 205 (it is hereafter described as Server S) outside a private network 202.

[0014] Since a transmitting partner's domain name knows the terminal A of a transmitting agency, the IP address is asked from the domain name (referred to as "ftp.out.co.jp") of Server S. The router 224 (it is hereafter described as Router K) to which Terminal A is connected asks an internetwork 201 side the IP address of the terminal (a server etc. is included) which has this domain name by the well-known approach through the router 203 (it is hereafter described as Router N) formed in the internetwork 201 side. Consequently, it replies to the formula IP address (it is referred to as "150.96.10.1" and written as "IP-D") with said domain name of Server S from an internetwork 201 side.

[0015] Supposing there shall be no address translation equipment 204 here and Router N notifies this formula IP address "150.96.10.1" to Terminal A through Router K, henceforth, Terminal A will set this IP address as the transmission place address in the header of the packet which transmits, and will be transmitted to it. However, since the terminal B in a private network 202 completely has the private IP address of the same number with IP-D in the example of drawing, when Terminal A sets "150.96.10.1" as the transmission place address, a packet may be transmitted to Terminal B.

[0016] Since such a situation is not produced, in drawing 24 , the address is changed in the address translation equipment 204 formed between the private network 202 and Router N. Only the address translation equipment 204 of the inside of a private network 202 is effective as the private address of Server S, and selects the private IP address (it is referred to as "159.99.30.1" and written as "IP-C") by which current use is not carried out in the private network 202, and notifies it to Terminal A while it will ask an internetwork 201 side the IP address

of Server S, if the IP packet which makes the domain name of Server S the transmission place address from Terminal A is received. Henceforth, Terminal A sets "IP-C" of a private IP address as the IP address of a transmission place, and transmits a packet.

[0017] Subsequently, if it replies to the formula IP address "150.96.10.1" of Server S from an internetwork 201 side to a previous inquiry, a formula IP address "IP-D" and a private IP address "IP-C" are made to correspond, and address translation equipment 204 memorizes them, changes into "IP-D" "IP-C" of the transmission place address of the packet transmitted from Terminal A, and sends it out to an internetwork 201 side.

[0018] On the other hand, since the private IP address (it is referred to as "154.100.10.1" and written as "IP-A") is given to Terminal A, this "IP-A" is set to the address of the transmitting origin of a packet. Since a private IP address is not accepted in an internetwork 201, address translation equipment 204 acquires a formula IP address (it is referred to as "150.47.1.1" and written as "IP-E") to Terminal A by the well-known approach, and memorizes correspondence of "IP-A" and "IP-E." Henceforth, "IP-A" set as the transmitting agency IP address of the packet transmitted from Terminal A is changed and transmitted to "IP-E."

[0019] Although it sets up the formula IP address "IP-E" of Terminal A as a transmission place IP address in transmitting a packet to Terminal A from Server S side, address translation equipment 204 changes into "IP-A" the transmission place address "IP-E" of the packet which received from Server S, and transmits it to a private network 202. Therefore, even if the terminal 225 which has the private IP address of the same number as the formula IP address "IP-E" of a transmission place in a private network 202 exists, a packet is not transmitted to the terminal.

(3) Although handshaking was explained to the subject next, explain the conventional address translation technique at the time of the terminal in the network (private network) which uses a private IP address performing an Internet connectivity beyond the IP address conversion approach about the conversion

approach of the address in the conventional technique.

[0020] Although address translation equipment is formed and address translation is performed in the above-mentioned example, generally the method of changing the address is learned for the conventional technique by making the technique called NAT and an IP masquarade (or multi-NAT) build in a router or a fire wall server.

[0021] NAT: Explain NAT (Network Address Translation) first. NAT is the address translation method specified by RFC1631, and is the function to change a private IP address and a global IP address. The router of a low price also has many which are characterized [one] by loading of this NAT function. Drawing 25 is drawing explaining an NAT function, and shows the network configuration and the model of the use gestalt of an IP address. In drawing 25 , a private IP address which was indicated all over drawing shall be given at each to two or more terminals 321 (in pointing out a specific terminal, it describes it as Terminal A etc.) connected to the private network (it is hereafter described as LAN) 320.

[0022] In such a configuration, in performing the Internet communication link (it connects with the terminal in other networks by which the illustration abbreviation was specifically carried out through global network 380) from the terminal A with the private IP address "10.1.1.10" connected to LAN320, Terminal A acquires "20.1.1.10" as a global IP address used by the Internet side through a router 310.

[0023] Although the router 310 builds in the NAT function, to the Internet side, a transmission place is changed into "10.1.1.10" of a private IP address by the NAT function by the NAT function in a router 310, and the packet in which "10.1.1.10" of a private IP address has the global IP address "20.1.1.10" of the transmission place address which is changed into "20.1.1.10" of a global IP address, and is sent from the Internet side is sent to Terminal A by Terminal A by it. Therefore, in this example, it becomes the form where "20.1.1.10" of a global IP address and "10.1.1.10" of a private IP address are used by corresponding. It can also be concluded that the conversion approach of an IP address explained by drawing 24 is an approach using NAT.

[0024] Thus, although the method of giving a global IP address at the time of connection, and making an Internet connectivity perform at it is called the terminal mold dial-up-IP connection service etc., since only the terminal which connects by this approach uses a global IP address, one global IP address can be used in common at two or more terminals 321 in LAN. However, since the number of the global IP addresses which one LAN320 can use for coincidence has become settled by the contract with JPNIC or its proxies (provider etc.) beforehand, the terminal more than the number cannot perform an Internet connectivity to coincidence. Moreover, since two or more terminals 221 share a global IP address, it cannot set a global IP address (for example, "20.1.1.10") as the transmission place address from the Internet side, and cannot specify the specific terminal in LAN320.

[0025] IP masquarade (multi-NAT):, next an IP masquarade (referred to also as multi-NAT) are explained. Although the IP masquarade also resembles NAT, to NAT changing conversion of a private IP address and a global IP address, i.e., an IP address part, an IP masquarade also uses a port number and performs address translation. As everyone knows, an IP address is located in the 3rd layer in an OSI reference model, and the transmission place address and the transmitting agency address are set up in IP header specified by RFC791. On the other hand, a port is given to the 5th-layer application correspondence which is equivalent to the most significant of an OSI reference model, and a port number is set up by the TCP protocol located in the 4th layer which hits the high order of IP layer (the 3rd layer). Therefore, a port number is not set up in IP header. Although assignment of a port number is locally performed by each host (terminal), if it does not know beforehand, about the port number used for application service that the first processing cannot be performed, the specific port number is defined fixed.

[0026] Drawing 26 and drawing 27 are drawings explaining an IP masquarade, drawing 26 shows a network configuration and the model of the use gestalt of an IP address, and drawing 27 shows an example of correspondence of a private IP

address and a global IP address. In the example of drawing 26 , a private IP address which was indicated all over drawing to each of two or more terminals 421 (it describes it as Terminal A etc. in pointing out a specific terminal) connected to the private network (it is described as LAN) 420 is given. Moreover, the port number currently used for a part of application used at each terminal 421 is indicated in this drawing. Although it is common that a multi-statement is carried out to one terminal since a port number is given to application correspondence, the port number "23" currently assigned to Telnet which is a kind of application fixed is used for all the terminals 421 by drawing, and the example with which the port number "21" currently assigned to Terminal E fixed at FTP (File Transfer Protocol) is used together is illustrated in it.

[0027] Although two or more terminals 421 share one global IP address (or defined number) also for an IP masquarade, the port number which can identify a terminal is set to a global IP address side. For example, in case an Internet connectivity is carried out to Terminal A - Terminal E, "20.1.1.10" is assigned to them by each as a global IP address, and also the port number according to individual is assigned to them for every combination of the private IP address of each terminal 421, and a port number (it corresponds to the class of application). The example of correspondence of the private IP address which contains a port number in drawing 27 , and a global IP address is described. In this example, when Telnet is used as application, "104" is assigned to Terminal E like ["100" and Terminal B] "101" and the following as a port number by the side of the Internet at Terminal A. When FTP is also used as application like Terminal E, a port number "105" is assigned to a port number "104" and FTP (port number by the side of a terminal "21") to Telnet (port number by the side of a terminal "23").

[0028]

[Problem(s) to be Solved by the Invention] As mentioned above, in NAT which is the conventional technique, or an IP masquarade, only an one direction communication link called access to the terminal which has a global address from the terminal which has a private address is realized. Neither access to the

terminal which has a private address from the terminal which has a global address, nor the communication link between two networks which have a private address was able to be performed. The global address newly needed to be acquired, it needed to assign the terminal which has a private address, and there was a trouble of requiring procedure and costs in these implementation.

[0029] Moreover, NAT and an IP masquarade had the trouble that only one direction communication service could be offered by the following skill constraint.

1. Since private address networks use the overlapping address space, respectively, they do not have the technique of uniformizing a terminal private address within the net.

2. The name resolution technique by current DNS does not have a means to acquire the IP address of a terminal private address within the net from a global address network.

3. There is no technique to which the router of a global address network treats the path information on a private address. That is, since there is no path of IP from a private address network to a global address network, a TCP connection cannot be stretched.

[0030] This invention is made in view of the above point, and the communication link to the terminal which has a private address is realized.

[0031]

[Means for Solving the Problem] It belongs to the 1st network which consists of this inventions with the communication device which has the address of the 1st type in order to solve the above-mentioned technical problem. In the communication device which has the 2nd network which consists of terminals which have the address of the 2nd type in the subordinate the identifier the terminal belonging to the network of the subordinate of other communication devices was named -- being concerned -- others -- with a means to manage corresponding to the identifier the communication device was named When the identifier the terminal used as a communications partner was named from a subordinate's terminal is received, the communication device characterized by

establishing a means to output the demand of address solution to the communication device which corresponds with said management tool is offered.

[0032] FQDN which is a unique identifier also to the terminal (node) which has the private address which is the address of the 2nd type here (fully-qualified domain name: a host name, a dot, a host's identifier constituted from three domain names'.) Assign www.fts.com etc., and match with the global address which is the address of the 1st type attached to other communication devices which have the terminal, and it manages. When the private address attached to the terminal which serves as a communications partner from a subordinate's terminal is received By specifying other corresponding communication devices and performing the solution demand of the address to other specified communication devices, a private address network and a global address network cannot be asked, but a unique identifier can be given to a terminal.

[0033] Moreover, the 1st network which consists of this inventions with the communication device which has the address of the 1st type in order to solve the above-mentioned technical problem, In the network system which consists of the 2nd network which consists of terminals which have the address of the 2nd type under the command of a communication device to said communication device The 1st management tool which the address of the subordinate's terminal is made to correspond with the identifier to which it was attached by each terminal, and manages it, The 2nd management tool which the identifier of a terminal is made to correspond with the communication device which manages the address of the terminal, and manages it, It asks for other communication devices which solve the address of the terminal of a communications partner to ****** and the communication link demand from a subordinate's terminal with said 2nd management tool, and the network system characterized by performing address solution with said 1st management tool with other communication devices is offered.

[0034] The 1st management tool of a communication device is the private address which is the 2nd address attached to a subordinate's terminal, and a

unique identifier here. FQDN is matched and managed. For example, the 2nd management tool When the identifier (FQDN) of a terminal and the global address which is the 1st address of the communication device which manages the terminal are matched and managed and a communication link demand is made from a subordinate's terminal Since the communication device which performs address solution with the 2nd management tool is specified and the 1st management tool of other communication devices was made to perform address solution, the name resolution of a private address is realizable via a global address network.

[0035] Furthermore, the global address network with which each node has the unique address in order to solve the above-mentioned technical problem in this invention, In the network system which has the private address network which has the address which is not unique, and address translation equipment which changes the address in case data are transmitted among these As opposed to each node to which said address translation equipment belongs to said private address network When the inquiry to a predetermined identifier is made from the predetermined node which gives and manages a unique identifier and belongs to said global address network or other private address networks The network system characterized by what a corresponding private address is acquired and notified for is offered.

[0036] Here, by assigning FQDN which is a unique identifier also to the node belonging to a private address network, a private address network and a global address network cannot be asked, but a terminal can have a unique identifier. Moreover, the DNS server for private address networks which does not belong to the tree of a DNS server global address within the net can be prepared for every private address network, and can realize the name resolution of a private address via a global address network by enabling it to access this from a global address network.

[0037] Moreover, the global address network with which each node has the unique address in order to solve the above-mentioned technical problem in this

invention, The private address network which has the address which is not unique, and the 1st address translation equipment which performs address translation in said global address network, In the network system which has the 2nd address translation equipment which performs address translation between said global address networks and said private address networks Said 1st and 2nd address translation equipment by establishing a connection independently, respectively and exchanging the information about a connection mutually between said global address network and said private network network The network system characterized by what transfer of data is enabled for is offered.

[0038] The 1st and 2nd address translation equipment establishes separately a connection private address within the net and a connection global address within the net here, and it becomes possible to realize the TCP connection from a global address network to a private address network because the 1st and 2nd address translation equipment exchanges information about both connections (map).

[0039]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing. In addition, a communication device says a node, for example, is a router. The address of the 1st type is a global address and the 2nd address is a private address.

[0040] Drawing 1 is drawing showing the example of a configuration of the gestalt of operation of this invention. As shown in this drawing, the gestalt of operation of this invention is constituted by terminal A-D, Routers A and B, and the DNS server.

[0041] Here, it connects mutually through Router A and Terminals A and B constitute the private address network. In addition, 192.168.0.2 is given to one side and Terminal B with which 192.168.0.1 is given to Terminal A as a private address as a private address.

[0042] While Router A transmits a packet among Terminals A and B, when transmitting a packet through a global address network, it performs address

translation. In addition, 34.56.10.4 which is a global address is given to Router A.
[0043] The DNS server holds the database which recorded the IP address of each node under management of the server, and correspondence of an identifier (host name), searches a database according to the inquiry from each node, and returns the result. Moreover, in retrieval of the host of the domain which is not in the bottom of management of it, it asks in a substitute to the DNS server (not shown) of a high order further, and it returns the result.
[0044] While Router B transmits a packet among Terminals C and D, when transmitting a packet through a global address network, it performs address translation. In addition, swan.mbb.nif.com which is 15.23.1.2 and the host name which are a global address is given to Router B.
[0045] It connects mutually through Router B and Terminals C and D constitute the private address network. In addition, PC-B.home-a.com is given to Terminal C as 192.168.0.2 and a host name as a private address. In addition, FQDN is adopted as a host name.
[0046] Drawing 2 is drawing showing the detailed example of a configuration of Router A and Router B. As shown in this drawing, Routers A and B In the IP section 10, the TCP section 11, the name resolution section 12, the solution-before private network address judging section 13, the name resolution server registration section 14 for communication link place private networks, the dummy IP address pool section 15, and the end of a communication link tip - gateway IP address / port attaching part 16, the packet transfer section 17, It is constituted by the address / port negotiation section 19 in the TCP connection management section 18 for a packet transfer, and the end of a communication link tip, and means of communications 20 and a console 21 are connected to the exterior.
[0047] Here, the IP section 10 is bearing the duty which transmits and receives the packet of TCP between two nodes. That is, a TCP packet is delivered between two nodes identified by the IP address. In addition, the IP section 10 has reception authorization IP address attaching part 10a holding the list of IP addresses to which reception is permitted.

[0048] The TCP section 11 establishes the connection who is a protocol for communicating between two applications. That is, first, a connection is established between applications and a bidirectional communication link is realized using the connection. In addition, the TCP section 11 has receive-port modification section 11a for changing a receive port.

[0049] The name resolution section 12 performs name resolution processing, when the name resolution demand by DNS is made. The solution-before private network address judging section 13 performs name resolution processing while checking the existence of the entry of the reference address to the name resolution server registration section 14 for communication link place private networks.

[0050] The name resolution server registration section 14 for communication link place private networks stores the information about the name resolution server for private networks. The dummy IP address pool section 15 holds a fixed number of dummy IP addresses used in case it communicates with the node belonging to a private network.

[0051] In case - gateway IP address / port attaching part 16 delivers and receives data between an accepting station and a transmit terminal, it registers the IP address and dummy IP address of each required node as an entry in the end of a communication link tip.

[0052] In case the packet transfer section 17 transmits a packet, it performs required processing. The TCP connection management section 18 for a packet transfer establishes a connection according to directions of the packet transfer section 17.

[0053] The address / port negotiation section 19 generates a Notification message and an ACK message, and transmits in the end of a communication link tip. Means of communications 20 is the physical layer including a transmission line, changes into a corresponding electrical signal the packet transmitted from other nodes, and supplies it to the IP section 10 while changing into a corresponding electrical signal the packet supplied from the IP section 10

and transmitting.

[0054] A console 21 is an interface at the time of registering information to the name resolution server registration section 14 for communication link place private networks. Next, actuation of the gestalt of the above operation is explained.

[0055] First, the name resolution processing at the time of the terminal A belonging to a private network accessing with reference to drawing 3 to the terminal C which similarly belongs to a private network is explained. First, data as shown in drawing 3 are registered through a console 21 to the name resolution server registration section 14 for communication link place private networks of Router A. That is, information "*. home-a.com//swan.mbb.nif.com" as shown in drawing 3 is registered into the name resolution server registration section 14 for communication link place private networks. As this information is shown in drawing 4 , it is the identifier by which the solution demand was carried out, and the information which consists of combination of the name resolution server of a solution reference, and is the identifier by which the solution demand of the *.home-a.com was carried out in the present example, and swan.mbb.nif.com is the identifier of the name resolution server of a solution reference. In addition, "*" shows a wild card and means the alphabetic character or character string of arbitration.

[0056] Next, in order to perform the inquiry to PC-B.home-a.com whose terminal A is the host name of Terminal C, it is DNS to Router A. If query is transmitted (refer to drawing 3), Router A will receive this data through means of communications 20, the IP section 10, and the TCP section 11, and will supply it to the name resolution section 12 through the transceiver port for name resolutions.

[0057] The name resolution section 12 transmits such a demand to the solution-before private network address judging section 13. The solution-before private network address judging section 13 searches the entry of the name resolution server registration section 14 for communication link place private networks,

checks the existence of the entry corresponding to this demand, and when an entry exists, it notifies the information about that entry to the name resolution section 12. Moreover, when an entry does not exist, it directs to perform the usual name resolution in the name resolution section 12.

[0058] The name resolution section 12 performs the usual name resolution processing, when performing the usual name resolution is directed. In being other, with reference to the information about an entry, it specifies the name resolution server of a solution reference. in order that the name resolution section 12 may acquire the address corresponding to a host name "swan.mbb.nif.com" first as shown in drawing 3 since the host name of the name resolution server of a solution reference is "swan.mbb.nif.com" and this supports Router B in the present example -- DNS query for"swan.mbb.nif.com" is transmitted to a DNS server. Consequently, from a DNS server, it is DNS. Since answer:15.23.1.2 are returned, Router A will know the address of Router B.

[0059] in order that the solution-before private network address judging section 13 which received the address may ask the IP address of the terminal C which is an accepting station to the router B which is the node which has the address "15.23.1.2" -- DNS query for"PC-B.home-a.com" is transmitted.

[0060] By the way, since the unique identifier is given and managed to Router B to the terminals C and D which exist in the subordinate, when there is such an inquiry, the IP address corresponding to the identifier is searched and returned. In the present example, the IP address "192.168.0.2" to Terminal C is acquired, and it is DNS. answer:192.168.0.2 will be returned.

[0061] Thus, the IP address of the acquired terminal C is supplied to the solution-before private network address judging section 13. In order to prevent that the acquired IP address is overlapped and used for other communication links, the solution-before private network address judging section 13 deletes the dummy IP address from the dummy IP address pool section 15, while acquiring one dummy IP address from the dummy IP address pool section 15. For example, in the present example, while a dummy address "10.0.0.1" is acquired, it will be deleted

from the dummy IP address pool section 15.

[0062] Then, the solution-before private network address judging section 13 transmits the acquired dummy IP address "10.0.0.1" to Terminal A as a reply of a name resolution demand. "10.0.0.1" which is a dummy IP address is transmitted without sending as a reply "192.168.0.2" which is the private address of Terminal C here because a private address may overlap between different private networks. So, with the gestalt of this operation, in order to avoid generating of such duplication, it is supposed that a router A subordinate's private address, i.e., the private address of a different class A from the private address of Class C, is used as a dummy IP address.

[0063] Suppose in the Internet that the IP address of the class A which is not usually used is used as a dummy IP address. Then, the solution-before private network address judging section 13 is registered as the address which may receive an IP address "10.0.0.1" to reception authorization IP address attaching part 10a. Consequently, the packet which includes an IP address "10.0.0.1" as the transmission place address will be permitted as an object of reception.

[0064] Next, the solution-before private network address judging section 13 registers as an entry the IP address of the terminal A which are the terminal C which is an accepting station, Router A, Router B, and a transmit terminal to - gateway IP address / port attaching part 16 in the end of a communication link tip. As shown in drawing 3 , specifically, "192.168.0.2-//34.56.10.4:??;15.23.1.2:??//192.168.0.1:??;10.0.0.1:??//x" will be registered as an entry. In addition, the port number determined by processing mentioned later is registered, and the last "x" is a communication link authorization flag, and "O" is registered into the part of "??" following an IP address when a communication link is not permitted, and a communication link is permitted for "x" again.

[0065] Next, with reference to drawing 5 , the processing in the case of establishing a TCP connection is explained. First, in order that Terminal A may establish the connection of TCP between the No. 23 ports of Terminal C to Router A, the SYN message of TCP is transmitted to the port of No. 23 of

10.0.0.1. Here, a source address is 192.168.0.1:YY (solvent-refined-coal=192.168.0.1:YY), as shown in drawing 5 .

[0066] Since 10.0.0.1 is registered into reception authorization IP address attaching part 10a, the IP section 10 of Router A receives this packet, and supplies it to the packet transfer section 17 through the TCP section 11.

[0067] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and acquires the entry corresponding to 10.0.0.1. Consequently, 10.0.0.1 is the course place of 15.23.1.2, and no port information becomes settled, and since a communication link authorization flag is in an off condition, this connection detects that it is in the condition which name resolution processing ended.

[0068] The packet transfer section 17 directs to establish a TCP connection between 192.168.0.2 via 15.23.1.2 to the TCP connection management section 18 for a packet transfer.

[0069] The packet transfer section 17 adds the source port address (YY) included in the SYN message, and a transmission place port (23) to the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip.

[0070] The TCP connection management section 18 for a packet transfer establishes a TCP connection through the TCP section 11 between the ports XX of 15.23.1.2. That is, the TCP connection management section 18 for a packet transfer transmits the SYN message of TCP to the port of No. 23 (solvent-refined-coal=192.168.0.1:YY) of 10.0.0.1 to Router B. Consequently, since "SYN+ACK" is returned from Router B, the TCP connection management section 18 for a packet transfer transmits "ACK" to Router B. In addition, XX is taken as the fixed port value of the arbitration beforehand assigned to these technique here. Consequently, a TCP connection will be established between Router B and Router A.

[0071] Next, the TCP connection management section 18 for a packet transfer registers into - gateway IP address / port attaching part 16 the connection

established between Routers B by the above processing in the end of a communication link tip. Namely, the TCP connection management section 18 for a packet transfer registers into - gateway IP address / port attaching part 16 WW and XX which are the transmitting agency port and transmission place port of TCP in the end of a communication link tip. Consequently, it will be changed into the port where "??" of the entry shown previously corresponds.

[0072] Next, the TCP connection management section 18 for a packet transfer directs in the end of a communication link tip that the Notification message (MSG) which shows "the port of No. 23 of 192.168.0.2" transmits from the TCP connection of Port WW to the port XX of 15.23.1.2 to the address / port negotiation section 19.

[0073] The address / port negotiation section 19 creates the Notification message which shows the port of No. 23 of 192.168.0.2, and transmits to Router B in the end of a communication link tip. Consequently, as shown in drawing 5 , a Notification message will be transmitted to Router B.

[0074] The TCP section 11 of Router B supplies the Notification message which received through Port XX to the packet transfer section 17. Since the packet transfer section 17 is the packet of the beginnings other than SYN transmitted from the transmit port WW, and ACK, it considers that this is a Notification message and transmits it to the TCP connection management section 18 for a packet transfer.

[0075] The TCP connection management section 18 for a packet transfer establishes a TCP connection between the addresses and the port numbers (No. 23 port of the address 192.168.10.2) which were shown in the Notification message. That is, the TCP connection management section 18 for a packet transfer transmits the SYN message of TCP to the port of No. 23 (solvent-refined-coal=192.168.0.1:YY) of 192.168.10.2 to Terminal C. Consequently, since "SYN+ACK" is returned from Terminal C, the TCP connection management section 18 for a packet transfer transmits "ACK" to Terminal C. Then, a connection will be established between Terminal C and Router B.

[0076] If a connection is established between Router B and Terminal C, Router B will require an ACK message as returning to Router A as a response to a Notification message.

[0077] Consequently, the address / port negotiation section 19 transmits the ACK message which notifies the completion of connection to the port of No. 23 of Terminal C (192.168.0.2) to Router A in the communication link tip end of Router B.

[0078] Then, the address / port negotiation section 19 stores the address information and port information about the newly established connection to - gateway IP address / port attaching part 16 in the end of a communication link tip in the communication link tip end of Router B. Namely, the address / port negotiation section 19 writes the entry which has the transmission place address of the newly established connection, a port (192.168.0.2:23) and a source address, the source address of the TCP connection to whom the port (10.0.0.1:ZZ) and the Notification message have been sent, a port (34.56.10.4:WW) and the transmission place address, a port (15.23.1.2:XX), and the communication link authorization flag of ON in - gateway IP address / port attaching part 16 in the end of a communication link tip in the end of a communication link tip.

[0079] Next, the address / port negotiation section 19 notifies that the port [of the address 192.168.0.2 / of No. 23] connection was established via the TCP connection from Port XX to the port WW of 34.56.10.4 of 15.23.1.2 to the TCP connection management section 18 for a packet transfer in the communication link tip end of Router A.

[0080] By using "34.56.10.4:WW;15.23.1.2:XX" as a key, the TCP connection management section 18 for a packet transfer searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and acquires the corresponding entry. And a connection with the terminal A over (referring to drawing 6) and the notified ACK message detects that it is 192.168.0.1:YY and 10.0.0.1:23 by referring to the information included in the acquired entry.

[0081] The TCP connection management section 18 for a packet transfer establishes a connection between 192.168.0.1:YY and 10.0.0.1:23 through the TCP section 11. That is, first, the TCP connection management section 18 for a packet transfer transmits SYN+ACK to Terminal A, and receives ACK returned from Terminal A as the result. Consequently, a connection will be established between Terminal A and Router A (refer to drawing 6).

[0082] And finally the TCP connection management section 18 for a packet transfer changes into ON (O) the communication link authorization flag of the entry "192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23" registered into - gateway IP address / port attaching part 16 in the end of a communication link tip from OFF (x) (refer to drawing 6).

[0083] Here, the entry registered into - gateway IP address / port attaching part 16 in the end of a communication link tip is constituted by an accepting station, an after [modification] transmission place IP address, an after [modification] transmission place port, an after [modification] transmission place IP address, an after [modification] transmission place port, a front [modification] transmission place IP address, a front [modification] transmission place port, a front [modification] transmitting former IP address, a front [modification] transmitting former port, and the communication link authorization flag as shown to drawing 7 .

[0084] In this example, a "accepting station" is the IP address (192.168.0.2) of Terminal C, and is information which only the router of the side which establishes a TCP connection on the Internet holds.

[0085] A "after [modification] transmitting former IP address" and "the transmitting former port after modification" are a transmitting agency IP address after address translation, and a transmitting agency port number. In this example, 34.56.10.4 which is the IP address of Router A, and a port number WW correspond.

[0086] A "after [modification] transmission place IP address" and a "after [modification] transmission place port" are the transmission place IP addresses

and transmission place port numbers after address translation. In this example, 15.23.1.2 which is the IP address of Router B, and a port number XX correspond.
[0087] A "front [modification] transmitting former IP address" and "the transmitting former port before modification" are a transmitting agency IP address before address translation, and a transmitting agency port number. In this example, 192.168.0.1 which is the IP address of Terminal A, and a port number YY correspond.
[0088] A "front [modification] transmission place IP address" and a "front [modification] transmission place port" are the transmission place IP addresses and transmission place port numbers before address translation. In this example, 10.0.0.1 which is a dummy IP address, and the port of No. 23 correspond.
[0089] A "communication link authorization flag" is information which shows whether the communication link is permitted to the entry concerned, and when the communication link of "x" and an one direction is made [in communication link authorization] in the case of "O" and disapproval, it becomes "**."
[0090] Next, the processing in the case of transmitting a packet with reference to drawing 8 using the TCP connection established by the above processing is explained. First, if the packet (TCP data to 10.0.0.1:23 (solvent-refined-coal=192.168.0.1:YY)) to which the header which shows that a transmission place is 10.0.0.1:23, and a transmitting agency is 192.168.0.1:YY was given is transmitted from Terminal A to Router A, Router A will receive this.
[0091] Since 10.0.0.1:23 is held at reception authorization IP address attaching part 10a, the IP section 10 of Router A receives this, and transmits it to the packet transfer section 17 through the TCP section 11.
[0092] The packet transfer section 17 acquires the entry which searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and corresponds. In the present example, the entry "192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23//O" shown in drawing 8 is acquired. And with reference to the information stored in this entry, 10.0.0.1:23 which is the transmission place IP address and port

information which are contained in the header of a packet is changed into 15.23.1.2:XX, and 192.168.0.1:YY which are a transmitting agency IP address and port information is changed into 34.56.10.4:WW. In addition, it does not change especially about the datagram of a packet.

[0093] The packet transfer section 17 transmits the packet which conversion of a header ended towards Router B through the TCP section 11. Router B receives the packet transmitted from Router A, reads it through Port XX, and is supplied to the packet transfer section 17.

[0094] The packet transfer section 17 acquires "NULL//10.0.0.1:ZZ;192.168.0.2:23//34.56.10.4:WW;15.23.1.2:XX//O" which is an entry corresponding to the packet which searched - gateway IP address / port attaching part 16 in the end of a communication link tip, and received. And the packet transfer section 17 changes into 192.168.0.2:23 15.23.1.2:XX which is the transmission place IP address and port information which are added to the header of a packet with reference to the information included in the acquired entry, and changes into 10.0.0.1:ZZ 192.168.0.1:YY which are a transmitting agency IP address and port information, and the datagram of a packet transmits it to Terminal C through the TCP section 11, without changing.

[0095] Consequently, the packet transmitted from Terminal A will reach the terminal C belonging to a private address network. Next, Terminal C generates the packet as a response to the packet which received, the transmission place IP address and port are set as 10.0.0.1:ZZ, and sets a transmitting agency IP address and a port as 192.168.10.2:23, and transmits it. In addition, 10.0.0.1:23 is used as a transmission place IP address for preventing distributing to other nodes of the private address network with which Terminal C belongs accidentally.

[0096] It is received by Router B and the packet transmitted from Terminal C is supplied to the IP section 10. Since 10.0.0.1:ZZ is held at reception authorization IP address attaching part 10a, the IP section 10 receives this packet and transmits it to the packet transfer section 17 through the TCP section 11.

[0097] The packet transfer section 17 acquires the entry which searches -

gateway IP address / port attaching part 16 in the end of a communication link tip, and corresponds. In the present example, "NULL//10.0.0.1:ZZ;192.168.0.2:23//34.56.10.4:WW;15.23.1.2:XX//O" shown in drawing 8 is acquired. And with reference to the information stored in this entry, 10.0.0.1:ZZ which is the transmission place IP address and port information which are contained in the header of a packet is changed into 34.56.10.4:WW, and 192.168.10.2:23 which is a transmitting agency IP address and port information is changed into 15.23.1.2:XX. In addition, it does not change especially about the datagram of a packet.

[0098] The packet transfer section 17 transmits the packet which conversion of a header ended towards Router A through the TCP section 11. Router A receives the packet transmitted from Router B, reads it through Port WW, and is supplied to the packet transfer section 17.

[0099] The packet transfer section 17 acquires "192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23//O" which is an entry corresponding to the packet which searched - gateway IP address / port attaching part 16 in the end of a communication link tip, and received. And the packet transfer section 17 changes into 192.168.0.1:YY 34.56.10.4:WW which is the transmission place IP address and port information which are added to the header of a packet with reference to the information included in the acquired entry, and changes into 10.0.0.1:23 15.23.1.2:XX which are a transmitting agency IP address and port information, and the datagram of a packet transmits it to Terminal A through the TCP section 11, without changing.

[0100] Consequently, the packet transmitted from Terminal C will reach the terminal A belonging to a private address network. It becomes possible to deliver and receive a packet by the above processings between Terminals A and Terminals C which belong to a private address network, respectively.

[0101] Next, with reference to drawing 9 and drawing 10 , the processing in the case of ending a TCP connection is explained. First, with reference to drawing 9 , the processing in the case of changing a bidirectional communication link into a

uni directional is explained.

[0102] If the FIN message of TCP is transmitted to the port of No. 23 (solvent-refined-coal=192.168.0.1:YY) of 10.0.0.1 in order to end a TCP connection from Terminal A, Router A will receive this message through a No. 23 port.

[0103] Since 10.0.0.1 which is the transmission place address added to the received header of a packet is stored in reception authorization IP address attaching part 10a, the IP section 10 of Router A judges it as a reception authorization packet, and is supplied to the packet transfer section 17 through the TCP section 11.

[0104] The packet transfer section 17 notifies that the FIN message came to the TCP connection management section 18 for a packet transfer from the TCP connection a transmission place IP address and whose port information are 10.0.0.1:23 and a transmitting agency IP address and whose port information are 192.168.0.1:YY(s).

[0105] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 15.23.1.2:XX 10.0.0.1:23 which is a transmission place IP address and port information, and changes into 34.56.10.4:WW 192.168.0.1:YY which are a transmitting agency IP address and port information, and the datagram of a packet transmits it to Router B via the TCP section 11, without changing.

[0106] If transmission of a packet is completed, - gateway IP address / port attaching part 16 will be searched in the end of a communication link tip, a transmission place IP address and a port will be 34.56.10.4:WW(s), and the TCP connection management section 18 for a packet transfer of Router A will wait for the ACK message which is a response message over the FIN message from the connection a transmitting agency IP address and whose port are 15.23.1.2:XX(s) to arrive.

[0107] It receives through Port XX and Router B supplies the packet transmitted from Router A to the packet transfer section 17. A transmission place IP address and a port are 15.23.1.2:XX(s), and the packet transfer section 17 notifies that

the FIN message arrived to the TCP connection management section 18 for a packet transfer from the TCP connection a transmitting agency IP address and whose port are 34.56.10.4:WW(s).

[0108] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, 15.23.1.2:XX which are a transmission place IP address and port information is changed into 192.168.0.2:23, 34.56.10.4.WW which are a transmitting agency IP address and port information is changed into 10.0.0.1:ZZ, and the datagram of a packet transmits a packet to Terminal C through the TCP section 11, without changing.

[0109] And - gateway IP address / port attaching part 16 is searched in the end of a communication link tip, a transmission place IP address port is 10.0.0.1:ZZ, and the TCP connection management section 18 for a packet transfer waits to return the ACK message to FIN from the connection whose transmitting agency IP address port is 192.168.0.2:23.

[0110] Then, Terminal C receives the FIN message transmitted from Router B, and transmits the ACK message of TCP which is the response to the port ZZ watch (solvent-refined-coal=192.168.10.2:23) of 10.0.0.1.

[0111] It receives through Port ZZ and Router B supplies the packet transmitted from Terminal C to the packet transfer section 17. A transmission place IP address and a port are 10.0.0.1:ZZ(s), and the packet transfer section 17 notifies that the ACK message arrived from the TCP connection who has a transmitting agency IP address and a port 192.168.10.2:23 to the TCP connection management section 18 for a packet transfer.

[0112] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 34.56.10.4:WW 10.0.0.1:ZZ which are a transmission place IP address and port information, it changes into 15.23.1.2:WW 192.168.10.2:23 which is a transmitting agency IP address and port information, and the datagram of a packet transmits it to Router A through the TCP section 11, without changing.

[0113] And the TCP connection management section 18 for a packet transfer

changes a communication link authorization flag into the corresponding entry "NULL//10.0.0.1:ZZ;192.168.0.2:23//34.56.10.4:WW;15.23.1.2:XX//O" which is stored in - gateway IP address / port attaching part 16 in the end of a communication link tip at "**" which shows an "one direction" from the condition of "communication link authorization."

[0114] Consequently, the connection between Terminal C and Router B is One-way. It will be in the condition of Connection. It receives through Port WW and Router A supplies the packet transmitted from Router B to the packet transfer section 17.

[0115] A transmission place IP address and a port are 34.56.10.4:WW(s), and the packet transfer section 17 notifies that the ACK message arrived to the TCP connection management section 18 for a packet transfer from the TCP connection a transmitting agency IP address and whose port are 15.23.1.2:XX(s).

[0116] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 192.168.0.1:YY 34.56.10.4:WW which are a transmission place IP address and port information, it changes into 10.0.0.1:23 15.23.1.2:XX which are a transmitting agency IP address and port information, and the datagram of a packet transmits it to Terminal A through the TCP section 11, without changing.

[0117] And the TCP connection management section 18 for a packet transfer is changed into "**" which shows an "one direction" from "O" which shows "communication link authorization" for the communication link authorization flag of the corresponding entry "192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23//O" which is stored in - gateway IP address / port attaching part 16 in the end of a communication link tip.

[0118] Consequently, the connection between Router B, Router A and Router A, and Terminal A is One-way. It will be in the condition of Connection. Next, with reference to drawing 10 , the processing in the case of terminating a TCP connection from a uni directional is explained.

[0119] If the FIN message of TCP is transmitted to the port ZZ watch (solvent-refined-coal=192.168.0.2:23) of 10.0.0.1 in order to end a TCP connection from Terminal C, Router B will receive this message through ZZ watch port.
[0120] Since 10.0.0.1 which is the transmission place address added to the received header of a packet is stored in reception authorization IP address attaching part 10a, the IP section 10 of Router B judges it as the packet of ability ready for receiving, and is supplied to the packet transfer section 17 through the TCP section 11.
[0121] The packet transfer section 17 notifies that the FIN message arrived to the TCP connection management section 18 for a packet transfer from the TCP connection a transmission place IP address and whose port information are 10.0.0.1:ZZ(s) and a transmitting agency IP address and whose port information are 192.168.0.2:23.
[0122] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 34.56.10.4:WW 10.0.0.1:ZZ which are a transmission place IP address and port information, and changes into 15.23.1.2:XX 192.168.0.2:23 which is a transmitting agency IP address and port information, and the datagram of a packet transmits it to Router A via the TCP section 11, without changing.
[0123] If transmission of a packet is completed, - gateway IP address / port attaching part 16 will be searched in the end of a communication link tip, a transmission place IP address and a port will be 15.23.1.2:XX(s), and the TCP connection management section 18 for a packet transfer of Router B will wait for the ACK message which is a response message over the FIN message from the connection a transmitting agency IP address and whose port are 34.56.10.4:WW(s) to arrive.
[0124] It receives through Port WW and Router A supplies the packet transmitted from Router B to the packet transfer section 17. A transmission place IP address and a port are 34.56.10.4:WW(s), and the packet transfer section 17 of Router A notifies that the FIN message arrived to the TCP connection management

section 18 for a packet transfer from the TCP connection a transmitting agency IP address and whose port are 15.23.1.2:XX(s).

[0125] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, 34.56.10.4:WW which are a transmission place IP address and port information is changed into 192.168.0.1:YY, 15.23.1.2:XX which are a transmitting agency IP address and port information is changed into 10.0.0.1:23, and the datagram of a packet transmits a packet to Terminal A through the TCP section 11, without changing.

[0126] And - gateway IP address / port attaching part 16 is searched in the end of a communication link tip, a transmission place IP address and a port are 10.0.0.1:23, and the TCP connection management section 18 for a packet transfer waits to return the ACK message to FIN from the connection whose transmitting agency IP address port is 192.168.0.1:YY.

[0127] a terminal -- A -- from -- FIN -- a message -- receiving -- a response -- ****** -- TCP -- ACK -- a message -- 10.0.0.1 -- a port -- 23 -- No. (solvent-refined-coal=192.168.0.1:YY) -- " -- transmitting -- having -- if -- Router A -- this -- receiving -- the packet transfer section 17 -- supplying .

[0128] A transmission place IP address and port information are 10.0.0.1:23, and the packet transfer section 17 notifies that the ACK message arrived from the TCP connection who has a transmitting agency IP address and port information 192.168.10.1:YY to the TCP connection management section 18 for a packet transfer.

[0129] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 15.23.1.2:XX 10.0.0.1:23 which is a transmission place IP address and port information, it changes into 34.56.10.4:WW 192.168.10.1:YY which are a transmitting agency IP address and port information, and the datagram of a packet transmits it to Router B through the TCP section 11, without changing.

[0130] And the TCP connection management section 18 for a packet transfer deletes the corresponding entry

"192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23//**" which is stored in - gateway IP address / port attaching part 16 in the end of a communication link tip.

[0131] Consequently, the connection between Terminal A and Router A is One-way. From the condition of Connection to Connection It will be in the condition of Close. Furthermore, the TCP connection management section 18 for a packet transfer of Router A notifies the dummy address indicated by the front [modification] transmission place IP address of an entry, i.e., the reception termination of 10.0.0.1, to reception authorization IP address attaching part 10a, and returns a dummy address to it at the dummy IP address pool section 15.

[0132] It receives through Port XX and Router B supplies the packet transmitted from Router A to the packet transfer section 17. A transmission place IP address and port information are 15.23.1.2:XX(s), and the packet transfer section 17 notifies that the ACK message arrived to the TCP connection management section 18 for a packet transfer from the TCP connection a transmitting agency IP address and whose port information are 34.56.10.4:WW(s).

[0133] The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 192.168.0.2:23 15.23.1.2:XX which are a transmission place IP address and port information, it changes into 10.0.0.1:ZZ 34.56.10.4:WW which are a transmitting agency IP address and port information, and the datagram of a packet transmits it to Terminal C through the TCP section 11, without changing.

[0134] And the TCP connection management section 18 for a packet transfer deletes the corresponding entry "192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23//**" which is stored in - gateway IP address / port attaching part 16 in the end of a communication link tip.

[0135] Consequently, the connection between Terminal C, and Router B and Router B and Router A is One-way. From the condition of Connection to Connection It will be in the condition of Close. Furthermore, the TCP connection

management section 18 for a packet transfer of Router B notifies the dummy address indicated by the transmitting former IP address after modification of an entry, i.e., the reception termination of 10.0.0.1, to reception authorization IP address attaching part 10a, and returns a dummy address to it at the dummy IP address pool section 15.

[0136] It becomes possible to end the once established connection by the above processing. Next, with reference to drawing 11 and drawing 12 , restoration processing when a TCP connection is cut by a certain cause is explained.

[0137] Drawing 11 is drawing explaining restoration processing when the connection between Router A and Router B cuts. If the connection between Router A and Router B cuts as shown in this drawing, the TCP section 11 of Router A and the TCP section 11 of Router B will detect what the connection cut.

[0138] The TCP section 11 of Router A which detected cutting of a connection notifies each IP address and port number of both ends (Router A and Router B) of the cut connection to the TCP connection management section 18 for a packet transfer.

[0139] By using as a key the data received from the TCP section 11, the TCP connection management section 18 for a packet transfer of Router A searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and clears the "communication link authorization flag" of the entry of a retrieval result. Moreover, since the "accepting-station" field is not NULL, self **** that it is the node which established TCP actively, and directs to establish a TCP connection between the ports XX of Router B in the TCP section 11.

[0140] Consequently, the TCP section 11 transmits the SYN message of TCP to the port XX watch (solvent-refined-coal=34.56.10.4:VV) of 15.23.1.2, in order to establish a connection to Router B.

[0141] At this time, by using as a key the data received from the TCP section 11, the TCP connection management section 18 for a packet transfer searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and clears the "communication link authorization flag" of the entry of a retrieval

result with Router B. Moreover, since the "accepting-station" field is NULL, self **** that it is not the node which established TCP actively, and waits for resetting of the connection from Router A.

[0142] And if the SYN message transmitted to Router B from Router A arrives, Router B will transmit a SYN+ACK message to Router A. Consequently, from Router A, an ACK message will be returned and the connection between these will be established again (Re-establishment).

[0143] If reestablishment of the connection between Router A and Router B is carried out, as for Router A, a Notification message will be transmitted like the above-mentioned case to Router B.

[0144] The router B which received the Notification message transmits ACK to a Notification message, rewrites the transmitting former port before modification of the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip to a new port number (VV), and sets a communication link authorization flag.

[0145] On the other hand, Router A receives an ACK message, rewrites the transmitting former port after transmitting modification of the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip to a new port number (VV), and sets a communication link authorization flag.

[0146] Even when the connection between Router A and Router B is cut by the above processing, reestablishment of the connection is carried out and it becomes possible to continue a communication link. Next, with reference to drawing 12 , restoration processing when the connection between Router B and Terminal C cuts is explained.

[0147] If the connection between Router B and Terminal C cuts by a certain cause, the TCP section 11 of Router B will detect this. The TCP section 11 of Router B notifies each IP address and port number of both ends (Router B and Terminal C) of the cut connection to the TCP connection management section 18 for a packet transfer.

[0148] By using as a key the data notified from the TCP section 11, the TCP connection management section 18 for a packet transfer searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and clears the "communication link authorization flag" of the entry of an inspection result. Moreover, between the ports of No. 23 of Terminal C, it directs in the TCP section 11 so that a TCP connection may be established.

[0149] Consequently, the SYN message of TCP is transmitted to the port of No. 23 (solvent-refined-coal=10.0.0.1:UU) of 192.168.0.2 from Router B to Terminal C.

[0150] Then, Terminal C receives this SYN message and answers a letter to Router B in the SYN+ACK message which is a response message. The router B which received the SYN+ACK message from Terminal C changes into a new port number (UU) the transmitting former port after modification of the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip, and changes a communication link authorization flag into the condition of ON while it transmits an ACK message to Terminal C.

[0151] It becomes possible to restore this and to continue a communication link by the above processing, even if it is the case where the connection between Router B and Terminal C cuts according to a certain cause. In addition, when a TCP connection is cut by a certain cause between Router A and Terminal A, restoration processing is performed similarly.

[0152] With reference to a flow chart, it explains that the processing finally performed in the gestalt of the operation explained above flows. Drawing 13 is a flow chart explaining the flow of the processing in the router A at the time of name resolution processing shown in drawing 2 being performed. This flow chart is processing performed when a name resolution demand reaches Router A, below, mentions as an example the case where a name resolution demand "PC-B.home.com" reaches Router A, and is explained.

[0153] Step S10: The name resolution section 12 receives "PC-B.home.com" which is the name resolution demand transmitted from Terminal A through

means of communications 20, the IP section 10, and the TCP section 11.

[0154] Step S11: The name resolution section 12 transmits this demand to the solution-before private network address judging section 13.

[0155] Step S12: Search the name resolution server registration section 14 for communication link place private networks, the solution-before private network address judging section 13 progresses to step S14, when it judges with judging and registering whether the entry of the reference address is registered, and when other, it progresses to step S13.

[0156] Step S13: The name resolution section 12 processes the demand received as a usual name resolution demand.

Step S14: The solution-before private network address judging section 13 directs that the IP address of Router B (swan.mbb.nifty.com) asks the predetermined DNS server of a global screen oversize to the name resolution section.

[0157] Step S15: The solution-before private network address judging section 13 receives the inquiry result (15.23.1.2) returned from the DNS server through means of communications 20, the IP section 10, the TCP section 11, and the name resolution section 12.

[0158] Step S16: The solution-before private network address judging section 13 directs that the IP address of an accepting station B (PC-B.home-a.com) asks 15.23.1.2 (router B) in the name resolution section 12.

[0159] Step S17: The solution-before private network address judging section 13 receives the inquiry result (192.168.0.2) returned from Router B through means of communications 20, the IP section 10, the TCP section 11, and the name resolution section 12.

[0160] Step S18: The solution-before private network address judging section 13 chooses the dummy IP address (for example, 10.0.0.1) of arbitration from the dummy IP address pool section 15, and deletes the address from the dummy IP address pool section.

[0161] Step S19: The solution-before private network address judging section 13 transmits to Terminal A as a reply of a name resolution demand of a dummy IP

address (10.0.0.1).

[0162] Step S20: The solution-before private network address judging section 13 directs that the packet which has a dummy IP address as the transmission place address receives from a private network side to reception authorization IP address attaching part 10a.

[0163] Step S21: The solution-before private network address judging section 13 registers Terminal B, Router A, Router B and each IP address of Terminal A, and a dummy IP address into - gateway IP address / port attaching part 16 as an entry in the end of a communication link tip. However, about a communication link authorization flag, it is set as an off condition.

[0164] Next, with reference to drawing 14 , the processing at the time of establishing a TCP connection is explained. In addition, between Router A and Router B, the processing in the case of establishing a TCP connection is mentioned as an example, and the following explanation explains it. The following steps will be started if SYN of TCP Terminal A to whose transmission place IP address is 10.0.0.1 and whose transmission place port is No. 23 reaches Router A.

[0165] Step S30: With reference to reception authorization IP address attaching part 10a, since the IP address "10.0.0.1" is registered, the IP section 10 of Router A receives this packet, and it supplies it to the packet transfer section 17 through the TCP section 11.

[0166] Step S31: The packet transfer section 17 searches a course place from - gateway IP address / port attaching part 16 in the end of a communication link tip. That is, the packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and detects that IP address 10.0.0.1 is in the course place of IP address 15.23.1.2. Moreover, no entry of port information is buried at this time, and since the communication link authorization flag is off, it detects that it is in the condition which the name resolution finished.

[0167] Step S32: The packet transfer section 17 directs to establish a TCP

connection between IP address 15.23.1.2 and IP address 192.168.0.2 to the TCP connection management section 18 for a packet transfer.

[0168] Step S33: The TCP connection management section 18 for a packet transfer establishes a TCP connection between the ports XX of IP address 15.23.1.2. Consequently, a connection will be established between Router B and Router A by processing between step S40 mentioned later.

[0169] Step S34: The TCP connection management section 18 for a packet transfer writes a transmission place port (WW and XX) in the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip the transmitting origin of TCP about the connection established in step S33.

[0170] Step S35: The TCP connection management section 18 for a packet transfer directs in the end of a communication link tip that the Notification message about the port of No. 23 of 192.168.0.2 transmits from the TCP connection of Port WW to the port XX of 15.23.1.2 in the address / port negotiation section 19.

[0171] Step S36: The address / port negotiation section 19 transmits the Notification message about the port of No. 23 of 192.168.0.2 to the port XX of 15.23.1.2 from the TCP connection of Port WW in the end of a communication link tip.

[0172] Step S40: Based on processing of step S33 mentioned above, a TCP connection is established also in Router B.

[0173] Step S41: The TCP section supplies the Notification message which received in Port XX to the packet transfer section 17. And since the packet transfer section 17 is the packet of the beginnings other than SYN transmitted from the transmit port WW, and ACK, it considers that this is a Notification message and supplies it to the TCP connection management section 18 for a packet transfer.

[0174] Step S42: The TCP connection management section 18 for a packet transfer establishes a TCP connection between the addresses and the ports (No.

23 of 192.168.10.2) which were shown by the Notification message.
[0175] Step S43: The TCP connection management section 18 for a packet transfer directs to transmit an ACK message to the port WW watch of 34.56.10.4 in the address / port negotiation section 19 in the end of a communication link tip, and is transmitted by the address / port negotiation section 19 through the already established TCP connection in the end of a communication link tip.
[0176] In the end of a communication link tip Step S44 : the address / port negotiation section 19 The transmission place address and the port (192.168.0.2:23) of TCP which were established, A source address, the source address of the TCP connection to whom the port (10.0.0.1:ZZ) and the Notification message have been sent, and a port (34.56.10.4:WW), The entry which has the transmission place address, a port (15.23.1.2:XX), and the communication link authorization flag of ON is written in - gateway IP address / port attaching part 16 in the end of a communication link tip, and it progresses to (1) of drawing 15 .
[0177] Then, a continuation of the above processing is explained with reference to drawing 15 . Step S50: The address / port negotiation section 19 notifies the purport which the port [of 192.168.0.2 / of No. 23] connection established via the TCP connection of Port XX to the port WW of 15.23.1.2 to the TCP connection management section 18 for a packet transfer in the communication link tip end of Router A.
[0178] Step S51: The TCP connection management section 18 for a packet transfer searches "34.56.10.4/WW;15.23.1.2:XX" for - gateway IP address / port attaching part 16 as a key in the end of a communication link tip, and detects that the TCP connections by the side of the transmit terminal of this are 192.168.0.1:YY and 10.0.0.1:23.
[0179] Step S52: The TCP connection management section 18 for a packet transfer establishes the TCP connection between 192.168.0.1:YY and 10.0.0.1:23 through the TCP section 11.
[0180] Step S53: The TCP connection management section 18 for a packet

transfer changes into ON the communication link authorization flag of the entry "192.168.0.2//34.56.10.4:WW;15.23.1.2:XX//192.168.0.1:YY;10.0.0.1:23" registered into - gateway IP address / port attaching part 16 in the end of a communication link tip.

[0181] The above processing enables it to establish a PCT connection between Router A and Router B. Next, the processing at the time of transmitting a packet with reference to drawing 16 using the TCP connection established by the above processings is explained. In addition, below, transfer processing of the packet between Router A and Router B is mentioned as an example, and is explained.

[0182] Step S60: The DATA packet of TCP whose transmission place address is 10.0.0.1 and whose transmission place port is No. 23 reaches Router A from Terminal A.

[0183] Step S61: Since 10.0.0.1 is registered into reception authorization IP address attaching part 10a, the IP section 10 of Router A receives this, and it carries out it through the TCP section 11, and pass it to the packet transfer section 17.

[0184] Step S62: The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, changes into 34.56.10.4:WW 192.168.0.1:YY which is transmitting agency IP address port information at 15.23.1.2:XX about 10.0.0.1:23 which is transmission place IP address port information, and leaves datagram of a packet intact.

[0185] Step S63: The packet transfer section 17 transmits the packet which conversion of the address ended through the TCP section 11.

[0186] Step S70: The DATA packet of TCP arrives at XX watch port of Router A to the router B.

[0187] Step S71: The TCP section 11 of Router B receives the DATA packet which arrived at Port XX, and passes it to the packet transfer section 17.

[0188] Step S72: The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, changes into 10.0.0.1:ZZ 192.168.0.1:YY which is transmitting agency IP address port

information 192.168.0.2:23 about 15.23.1.2:XX which are a transmission place IP address and port information, and leaves datagram of a packet intact.

[0189] Step S73: The packet transfer section 17 transmits the packet which conversion of the address ended to PC-B.home-a.com (terminal C) through the TCP section 11.

[0190] The above processing enables it to transmit a packet using a TCP connection. Next, with reference to drawing 17 , in case a TCP connection is ended, the processing performed in Router A and Router B is explained.

[0191] Step S80: Terminal A to the transmission place address is 10.0.0.1, and the FIN packet of TCP whose transmission place port is No. 23 reaches Router A.

[0192] Step S81: Since 10.0.0.1 is registered into reception authorization IP address attaching part 10a, the IP section 11 of Router A receives this, and it passes it to the packet transfer section 17 through the TCP section 11. And processing of step S83 and step S82 is performed in parallel.

[0193] Step S82: - gateway IP address / port attaching part 16 is searched in the end of a communication link tip, the TCP connection management section 18 for a packet transfer judges whether the ACK message to FIN from the connection whose transmission place IP address port is 34.56.10.4.WW and whose transmitting agency IP address port is 15.23.1.2:XX was received, when it receives, it progresses to (2) of drawing 18 , and when other, it repeats the same processing.

[0194] Step S83: The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, changes into 34.56.10.4:WW 192.168.0.1:YY which is transmitting agency IP address port information at 15.23.1.2:XX about 10.0.0.1:23 which is transmission place IP address port information, and the datagram of a packet considers as a condition as it is, and it transmits it to Router B through the TCP section 11.

[0195] Step S90: The FIN packet of TCP arrives at XX watch port of Router B from Router A.

Step S91: The TCP section 11 passes the FIN packet which received in Port XX

to the packet transfer section 17. And in the TCP connection management section 18 for a packet transfer, the packet transfer section 17 performs processing of step S92 and step S93 in parallel, after notifying that the TCP connection a transmission place IP address and whose port are 15.23.1.2:XX(s) and a transmitting agency IP address and whose port are 34.56.10.4.WW(s) to FIN arrived.

[0196] Step S92: - gateway IP address / port attaching part 16 is searched in the end of a communication link tip, the TCP connection management section 18 for a packet transfer judges whether the ACK message to FIN from the connection a transmission place IP address and whose port are 10.0.0.1.ZZ(s) and a transmitting agency IP address and whose port are 192.168.0.2.23 was received, when received, it progresses to (3) of drawing 18 , and when other, it repeats the same processing.

[0197] Step S93: The packet transfer section 17 searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes into 10.0.0.1:ZZ 34.56.10.4.WW which are a transmitting agency IP address and port information 192.168.0.2:23 about 15.23.1.2:XX which are a transmission place IP address and port information, and the datagram of a packet transmits it to PC-B.home-a.com through the TCP section 11, without changing.

[0198] Then, a continuation of the above processing is explained with reference to drawing 18 . Step S100: The same actuation as Router B, i.e., processing of the below-mentioned steps S110-S117, performs modification or deletion of the entry of - gateway IP address / port attaching part 16 in a transfer of an ACK packet, and the end of a communication link tip.

[0199] Step S110: An ACK packet reaches Router B.

Step S111: Since the address 10.0.0.1 included in the ACK packet is registered into reception authorization IP address attaching part 10a, it receives this, and it passes the IP section 10 of Router B to the packet transfer section 17 through the TCP section 11.

[0200] Step S112: The packet transfer section 17 notifies that ACK arrived to the

TCP connection management section 18 for a packet transfer from the TCP connection a transmission place IP address and whose port are 10.0.0.1:ZZ(s) and a transmitting agency IP address and whose port are 192.168.0.2:23.

[0201] Step S113: It identifies that the TCP connection management section for a packet transfer is ACK for which it was waiting at step S92 of drawing 17 , and the TCP connection management section 18 for a packet transfer searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and the communication link authorization flag of the entry corresponding to this progresses [ON (O) and one-way (**) are judged and, in one-way, it progresses at step S114, and] to step S116, in being other.

[0202] Step S114: Transmit an ACK packet to Router B based on an approach [finishing / explanation / already].

Step S115: The TCP connection management section 18 for a packet transfer deletes the entry stored in - gateway IP address / port attaching part 16 in the end of a communication link tip. Moreover, at this time, the TCP connection management section 18 for a packet transfer notifies the reception termination of the dummy address indicated by the transmitting former IP address after modification of an entry to reception authorization IP address attaching part 10a, and returns a dummy address to it at the dummy IP address pool section 15.

[0203] Step S116: Transmit an ACK packet to Router B based on an approach [finishing / explanation / already].

Step S117: The TCP connection management section 18 for a packet transfer makes a setting change of the communication link authorization flag of the entry stored in - gateway IP address / port attaching part 16 in the end of a communication link tip at One-way.

[0204] The above processing enables it to end a TCP connection. Next, with reference to drawing 19 , restoration processing when a TCP connection cuts is explained. In addition, below, restoration processing when the connection between Router A and Router B cuts is mentioned as an example, and is explained.

[0205] Step S120: The TCP section 11 of Router A detects what the TCP connection of a between [Routers B] cut.
[0206] Step S121: The TCP section 11 of Router A notifies each IP address and port number of both ends (Router A and Router B) which are the connection who cut to the TCP connection management section 18 for a packet transfer.
[0207] Step S122: By using as a key the data received from the TCP section 11, the TCP connection management section 18 for a packet transfer of Router A searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and clears the "communication link authorization flag" of the entry of a retrieval result.
[0208] Step S123: Since the field is not NULL in "the end of a transmitting tip", the TCP connection management section 18 for a packet transfer of Router A directs to establish a TCP connection in the TCP section 11 between the ports XX of Router B.
[0209] Step S124: Transmit a Notification message based on an approach [finishing / explanation / already].
[0210] Step S125: Receive an ACK message based on an approach [finishing / explanation / already].
Step S126: The TCP connection management section 18 for a packet transfer rewrites the transmitting former port after transmitting modification of an entry to a new port number (VV).
[0211] Step S127: The packet transfer section 17 sets a communication link authorization flag.
Step S130: The TCP section of Router B detects TCP connection ** of a between [Routers A].
[0212] Step S131: The TCP section 11 of Router B notifies each IP address and port number of both ends (Router A and Router B) of the connection who cut to the TCP connection management section 18 for a packet transfer.
[0213] Step S132: By using as a key the data received from the TCP section 11, the TCP connection management section 18 for a packet transfer of Router B

searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes the "communication link authorization flag" of the entry of a retrieval result into an off condition.

[0214] Step S133: Since the field is NULL in "the end of a transmitting tip", the TCP connection management section 18 for a packet transfer of Router B waits for resetting of the connection from Router A.

[0215] Step S134: Receive the Notification message transmitted in step S124.

[0216] Step S135: Transmit the ACK message to a Notification message based on an approach [finishing / explanation / already].

[0217] Step S136: The TCP connection management section 18 for a packet transfer rewrites the transmitting former port before modification of the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip to a new port number (VV).

[0218] Step S137: The TCP connection management section 18 for a packet transfer sets the communication link authorization flag of an entry with which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip.

[0219] A connection can be restored when the connection between Router A and Router B cuts by the above processing. Next, with reference to drawing 20 , restoration processing when the connection between Router B and Terminal C cuts is explained.

[0220] Step S140: The TCP section 11 of Router B detects what the connection between Terminals C cut.

[0221] Step S141: The TCP section 11 of Router B notifies each IP address and port number of both ends (Router B and Terminal C) of the connection who cut to the TCP connection management section 18 for a packet transfer.

[0222] Step S142: By using as a key the data received from the TCP section 11, the TCP connection management section 18 for a packet transfer of Router B searches - gateway IP address / port attaching part 16 in the end of a communication link tip, and changes the communication link authorization flag of

the entry of a retrieval result into an off condition.

[0223] Step S143: The TCP connection management section 18 for a packet transfer of Router B directs to establish a TCP connection in the TCP section 11 between the ports of No. 23 of Terminal C. Consequently, call origination of the TCP connection is carried out.
 [0224] Step S144: The TCP connection management section 18 for a packet transfer of Router B changes the entry to which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip. That is, a transmitting agency port is rewritten to a new port number (UU).

[0225] Step S145: The TCP connection management section 18 for a packet transfer of Router B changes into the condition of ON the communication link authorization flag of an entry with which - gateway IP address / port attaching part 16 corresponds in the end of a communication link tip. Consequently, a TCP connection will be established between Terminals B.

[0226] Even when the TCP connection between Router B and Terminal C cuts by the above processing, it becomes possible to restore a connection. According to [as explained above] this invention, it is unique FQDN (fully-qualified domain name: a host name, a dot, a host's identifier constituted from three domain names'.). Since www.fts.com etc. was assigned to the terminal private address within the net, a private address network and a global address network cannot be asked, but a terminal can have a unique identifier. Consequently, although private address networks use the overlapping address space, respectively, it becomes possible to uniformize a terminal private address within the net.

[0227] Moreover, since the DNS server for private address networks which does not belong is prepared for the tree of a DNS server global address within the net for every private address network and it enabled it to access this from a global address network according to this invention, it becomes possible to realize the name resolution of a private address via a global address network.

[0228] Furthermore, according to this invention, a private network and a global network boundary router (address translation equipment) stretch separately a

TCP connection private address within the net and a TCP connection global address within the net, and it becomes possible to realize the TCP connection from a global address network to a private address network because a router carries out the map (information interchange) of both the connections.

[0229] (Additional remark 1) In the communication device which has the 2nd network which consists of terminals which belong to the 1st network which consists of communication devices which have the address of the 1st type, and have the address of the 2nd type in the subordinate the identifier the terminal belonging to the network of the subordinate of other communication devices was named -- being concerned -- others -- with a means to manage corresponding to the identifier the communication device was named The communication device characterized by establishing a means to output the demand of address solution to the communication device which corresponds with said management tool when the identifier the terminal used as a communications partner was named from a subordinate's terminal is received.

[0230] (Additional remark 2) a means to make the address of the subordinate's terminal correspond with the identifier to which it was attached by the terminal, and to manage it -- said -- others -- the demand of the address solution of the terminal of the subordinate from a communication device -- receiving -- said management tool -- the address -- solving -- said -- others -- communication device of the additional remark 1 publication characterized by establishing a means to notify the address solved to the communication device.

[0231] (Additional remark 3) the demand of address solution -- receiving -- the notice of solution of the address -- said -- others, when it receives from a communication device A means to match the address which received the notice with the dummy address which is said 2nd type of address and was changed into the address which is not used as the address of the terminal the subordinate's network, and to manage it, The communication device of the additional remark 2 publication characterized by establishing a means to notify said address after conversion to the terminal which required the communication link.

[0232] (Additional remark 4) the case where a packet with the dummy address after a notice is received from the terminal which required the communication link -- a dummy address -- said -- others -- communication device of the additional remark 3 publication characterized by establishing a means to change into the address of a communication device.

[0233] (Additional remark 5) The 1st network which consists of communication devices which have the address of the 1st type, In the network system which consists of the 2nd network which consists of terminals which have the address of the 2nd type under the command of a communication device to said communication device The 1st management tool which the address of the subordinate's terminal is made to correspond with the identifier to which it was attached by each terminal, and manages it, The 2nd management tool which the identifier of a terminal is made to correspond with the communication device which manages the address of the terminal, and manages it, The network system characterized by asking for other communication devices which solve the address of the terminal of a communications partner to ****** and the communication link demand from a subordinate's terminal with said 2nd management tool, and performing address solution with said 1st management tool with other communication devices.

[0234] (Additional remark 6) The global address network with which each node has the unique address, In the network system which has the private address network which has the address which is not unique, and address translation equipment which changes the address in case data are transmitted among these As opposed to each node to which said address translation equipment belongs to said private address network When the inquiry to a predetermined identifier is made from the predetermined node which gives and manages a unique identifier and belongs to said global address network or other private address networks The network system characterized by what a corresponding private address is acquired and notified for.

[0235] (Additional remark 7) other address translation equipments arranged at

the transmit-terminal side -- further -- having -- said -- others -- network system of the additional remark 6 publication characterized by registering into address translation equipment beforehand the unique identifier given to each node.

[0236] (Additional remark 8) The global address network with which each node has the unique address, The private address network which has the address which is not unique, and the 1st address translation equipment which performs address translation in said global address network, In the network system which has the 2nd address translation equipment which performs address translation between said global address networks and said private address networks Said 1st and 2nd address translation equipment by establishing a connection independently, respectively and exchanging the information about a connection mutually between said global address network and said private network network The network system characterized by what transfer of data is enabled for.

[0237] (Additional remark 9) Said 1st address translation equipment is the network system of the additional remark 8 publication characterized by notifying the information about said connection to said 2nd address translation equipment in case a transmit terminal establishes a connection.

[0238] (Additional remark 10) For the actual private address of an accepting station, said 1st address translation equipment is the network system of the additional remark 9 publication characterized by notifying the address of a different dummy to said transmit terminal.

[0239] (Additional remark 11) For the actual private address of said accepting station, the address of said dummy is the network system of the additional remark 10 publication characterized by being the address with which network classes differ.

[0240] (Additional remark 12) Said 2nd address translation equipment is the network system of the additional remark 9 publication characterized by reestablishing a connection again with reference to the information about said connection notified from said 1st address translation equipment when the connection between said accepting stations is cut.

[0241] (Additional remark 13) Said 1st address translation equipment When the connection between said 2nd address translation equipment is cut While newly carrying out connection establishment between said 2nd address translation equipment with reference to the information about an accepting station The information about said connection is notified to said 2nd address translation equipment. Said 2nd address translation equipment The network system of the additional remark 9 publication characterized by what a connection is updated for based on the information about said connection notified from said 1st address translation equipment.

[0242] (Additional remark 14) Said 1st and 2nd address translation equipment is the network systems of the additional remark 9 publication characterized by holding the information which shows a connection's condition and transmitting data based on this information.

[0243] (Additional remark 15) The information which shows said connection's condition is the network system of the additional remark 9 publication characterized by being the information only a uni directional indicates either which can communicate to be finishing [establishment] during establishment of a connection.

[0244] (Additional remark 16) The global address network with which each node has the unique address, In the address translation equipment which changes the address in case data are transmitted between the private address networks which have the address which is not unique A unique identifier is given and managed to each node belonging to said private address network. Address translation equipment characterized by what a corresponding private address is acquired and notified for when the inquiry to a predetermined identifier is made from the predetermined node belonging to said global address network or other private address networks.

[0245] (Additional remark 17) The global address network with which each node has the unique address, It connects with the network which has other address translation equipments which perform address translation between the private

address network which has the address which is not unique, and said global address network and said private address network. In the address translation equipment which performs address translation in said global address network said -- others -- address translation equipment -- independent -- a connection -- being established -- said -- others -- by exchanging the information about a connection mutually between address translation equipment Address translation equipment characterized by enabling transfer of data between said global address network and said private network network.

[0246] (Additional remark 18) the information concerning said connection in case, as for said address translation equipment, a transmit terminal establishes a connection -- said -- others -- address translation equipment of the additional remark 17 publication characterized by what is notified to address translation equipment.

[0247] (Additional remark 19) For the actual private address of an accepting station, said address translation equipment is address translation equipment of the additional remark 18 publication characterized by notifying the address of a different dummy to a transmit terminal.

[0248] (Additional remark 20) For the actual private address of said accepting station, the address of said dummy is address translation equipment of the additional remark 19 publication characterized by being the address with which network classes differ.

[0249]

[Effect of the Invention] It belongs to the 1st network which consists of this inventions with the communication device which has the address of the 1st type as explained above. In the communication device which has the 2nd network which consists of terminals which have the address of the 2nd type in the subordinate the identifier the terminal belonging to the network of the subordinate of other communication devices was named -- being concerned -- others -- with a means to manage corresponding to the identifier the communication device was named Since a means to output the demand of address solution to the

communication device which corresponds with a management tool was established when the identifier the terminal used as a communications partner was named from a subordinate's terminal was received A private address network and a global address network cannot be asked, but a unique identifier can be given to a terminal.

[0250] Moreover, the 1st network which consists of this inventions with the communication device which has the address of the 1st type as explained above, In the network system which consists of the 2nd network which consists of terminals which have the address of the 2nd type under the command of a communication device to a communication device The 1st management tool which the address of the subordinate's terminal is made to correspond with the identifier to which it was attached by each terminal, and manages it, The 2nd management tool which the identifier of a terminal is made to correspond with the communication device which manages the address of the terminal, and manages it, Since it asks for other communication devices which solve the address of the terminal of a communications partner to ****** and the communication link demand from a subordinate's terminal with the 2nd management tool and the 1st management tool was made to perform address solution with other communication devices A unique identifier is given to a terminal and the thing [communicating by being based on identifying] becomes possible.

[0251] Moreover, the global address network with which each node has the unique address in this invention as explained above, In the network system which has the private address network which has the address which is not unique, and address translation equipment which changes the address in case data are transmitted among these As opposed to each node to which address translation equipment belongs to a private address network When the inquiry to a predetermined identifier is made from the predetermined node which gives and manages a unique identifier and belongs to a global address network or other private address networks Since a corresponding private address is acquired and it was made to notify, the exception of a private address network or a global

address network is not asked, but it enables each node to have a unique identifier.

[0252] Furthermore, the global address network with which each node has the unique address in this invention, The private address network which has the address which is not unique, and the 1st address translation equipment which performs address translation in a global address network, In the network system which has the 2nd address translation equipment which performs address translation between a global address network and a private address network The 1st and 2nd address translation equipment by establishing a connection independently, respectively and exchanging the information about a connection mutually between a global address network and a private network network Since it was made to enable transfer of data, it becomes possible to establish the connection from a global address network to a private address network.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the gestalt of operation of this invention.

[Drawing 2] It is drawing showing the detailed example of a configuration of a router.
[Drawing 3] It is a signal flow Fig. explaining the name resolution processing at the time of the terminal A belonging to a private network accessing to the terminal B which similarly belongs to a private network.
[Drawing 4] It is drawing explaining a format of the information registered into the name resolution server registration section for communication link place private networks.
[Drawing 5] It is a signal flow Fig. explaining the processing in the case of establishing a TCP connection.
[Drawing 6] It is a signal flow Fig. explaining the processing in the case of establishing a TCP connection.
[Drawing 7] It is drawing explaining a format of the entry registered into - gateway IP address / port attaching part in the end of a communication link tip.
[Drawing 8] It is a signal flow Fig. explaining the processing in the case of transmitting a packet using a TCP connection.
[Drawing 9] In case a TCP connection is ended, it is a signal flow Fig. explaining the processing in the case of changing a bidirectional communication link into a uni directional.
[Drawing 10] In case a TCP connection is ended, it is a signal flow Fig. explaining the processing in the case of ending the communication link of a uni directional.
[Drawing 11] When the connection between Router A and Router B cuts, it is a signal flow Fig. explaining the processing at the time of restoring this.
[Drawing 12] When the connection between Router B and Terminal C cuts, it is a signal flow Fig. explaining the processing at the time of restoring this.
[Drawing 13] It is a flow chart explaining the flow of the processing in the router A at the time of name resolution processing being performed.
[Drawing 14] It is a flow chart explaining the processing at the time of establishing a TCP connection.
[Drawing 15] It is a flow chart explaining the processing at the time of

establishing a TCP connection.

[Drawing 16] It is a flow chart explaining the processing at the time of transmitting a packet using the TCP connection established by processing of drawing 14 and drawing 15 .

[Drawing 17] In case a TCP connection is ended, it is a flow chart explaining the processing performed in Router A and Router B.

[Drawing 18] In case a TCP connection is ended, it is a flow chart explaining the processing performed in Router A and Router B.

[Drawing 19] It is a flow chart explaining restoration processing when a TCP connection cuts.

[Drawing 20] It is a flow chart explaining restoration processing when the connection between Router B and Terminal C cuts.

[Drawing 21] It is drawing showing the configuration of the IP address of each class.

[Drawing 22] It is drawing for explaining the range of the figure used for the IP address of each class.

[Drawing 23] It is drawing showing the numeric value of the private IP address specified to RFC1597.

[Drawing 24] It is drawing having summarized, added and shown the contents of explanation of this official report in the block diagram of the internetwork environment indicated by drawing 1 indicated in the official report.

[Drawing 25] It is drawing explaining an NAT function.

[Drawing 26] It is drawing showing the network configuration and the model of the use gestalt of an IP address in an IP masquarade.

[Drawing 27] It is drawing showing an example of correspondence of the private IP address in an IP masquarade, and a global IP address.

[Description of Notations]

10 The IP Section

10a Reception authorization IP address attaching part

11 The TCP Section

11a Receive-port modification section

12 Name Resolution Section

13 Solution-before Private Network Address Judging Section

14 Name Resolution Server Registration Section for Communication Link Place Private Networks

15 Dummy IP Address Pool Section

16 The End of Communication Link Tip and Gateway IP Address / Port Attaching Part

17 Packet Transfer Section

18 TCP Connection Management Section for Packet Transfer

19 The End Address of Communication Link Tip / Port Negotiation Section

20 Means of Communications

21 Console

[Translation done.]

* NOTICES *

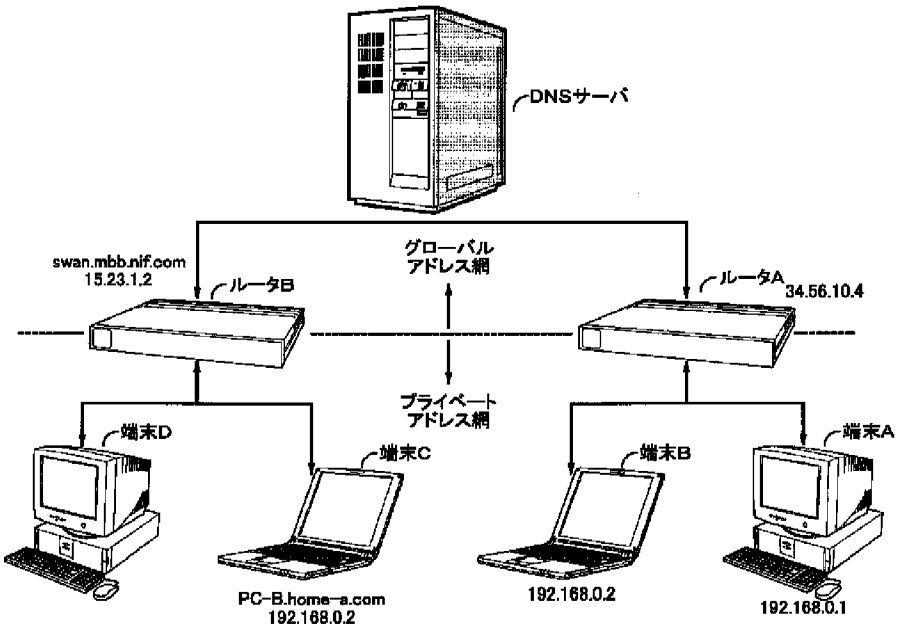
1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

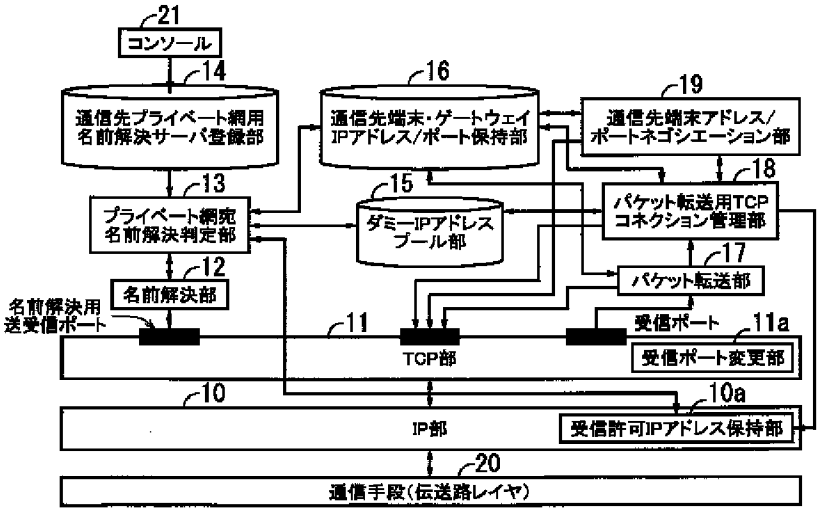
3.In the drawings, any words are not translated.

DRAWINGS

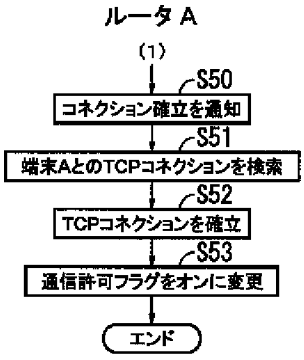
[Drawing 1]



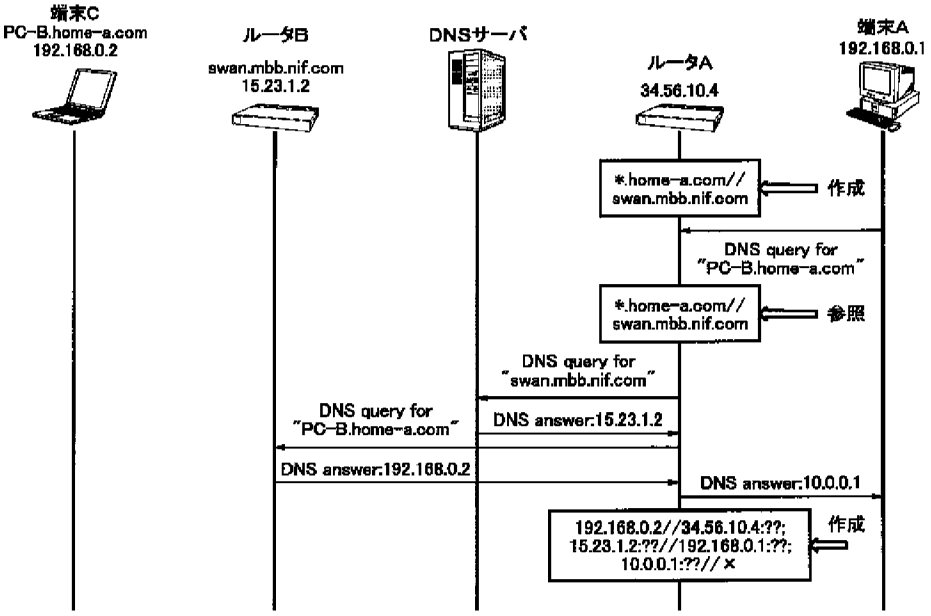
[Drawing 2]



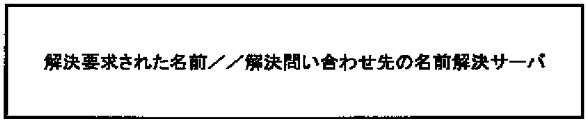
[Drawing 15]



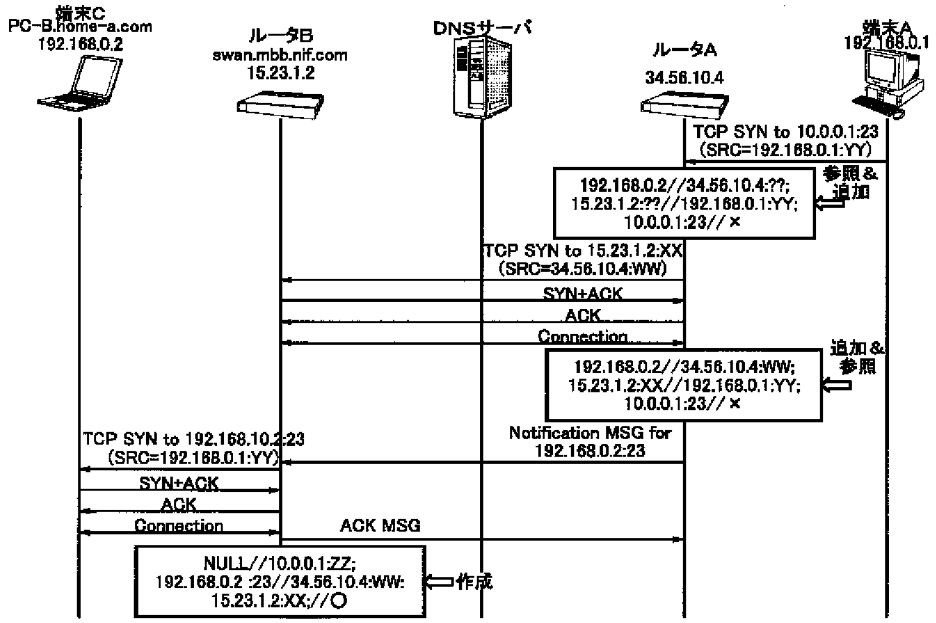
[Drawing 3]



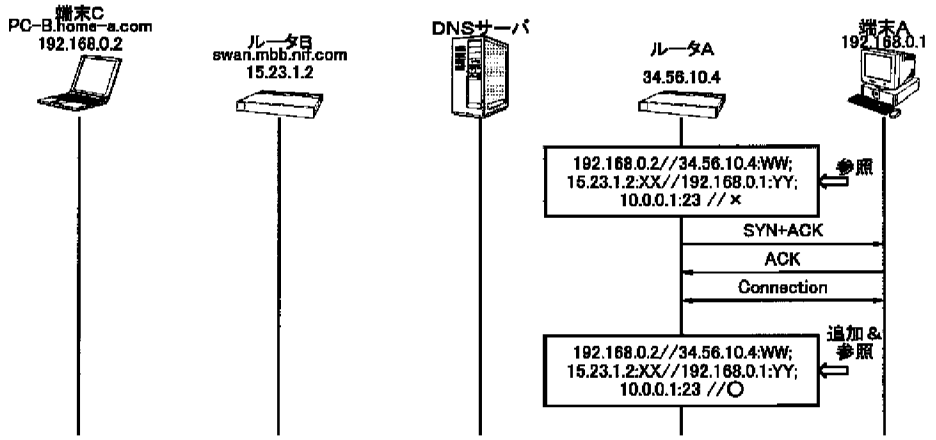
[Drawing 4]



[Drawing 5]



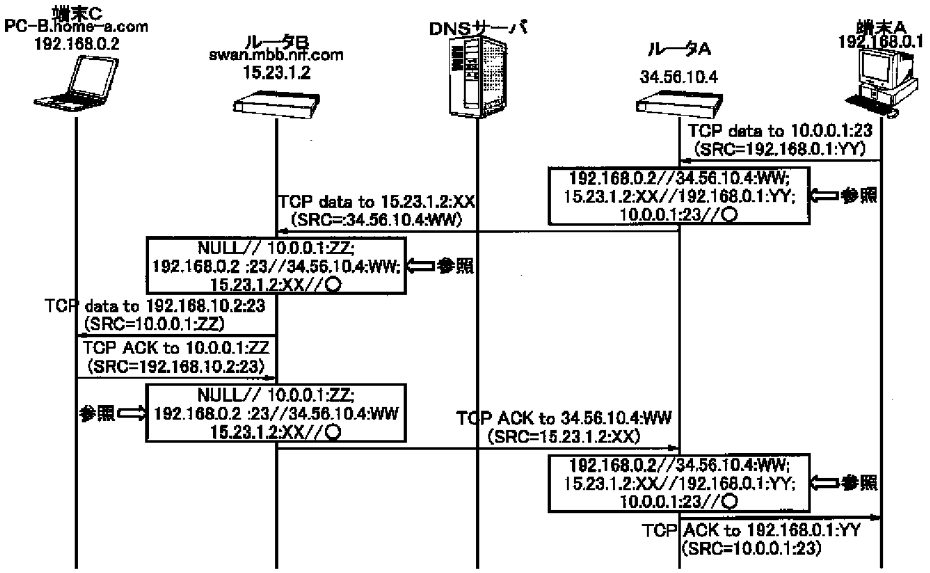
[Drawing 6]



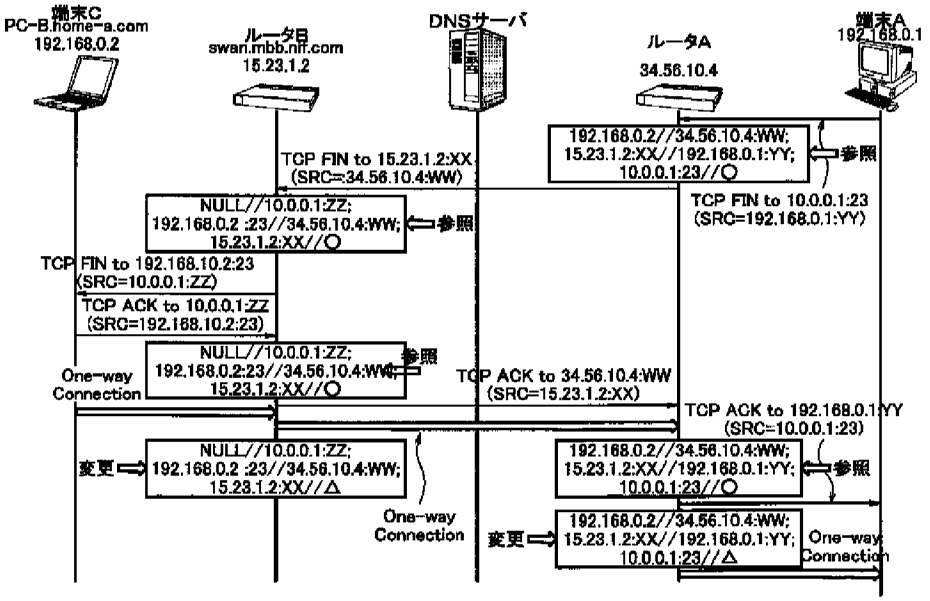
[Drawing 7]

受信端末(インターネット上のTCPのコネクションを確立する側のルータのみ保持)／／
変更後送信元IPアドレス:変更後送信元ポート:変更後送信先IPアドレス:変更後送信先ポート／／
変更前送信元IPアドレス:変更前送信元ポート:変更前送信先IPアドレス:変更前送信先ポート／／
通信許可フラグ

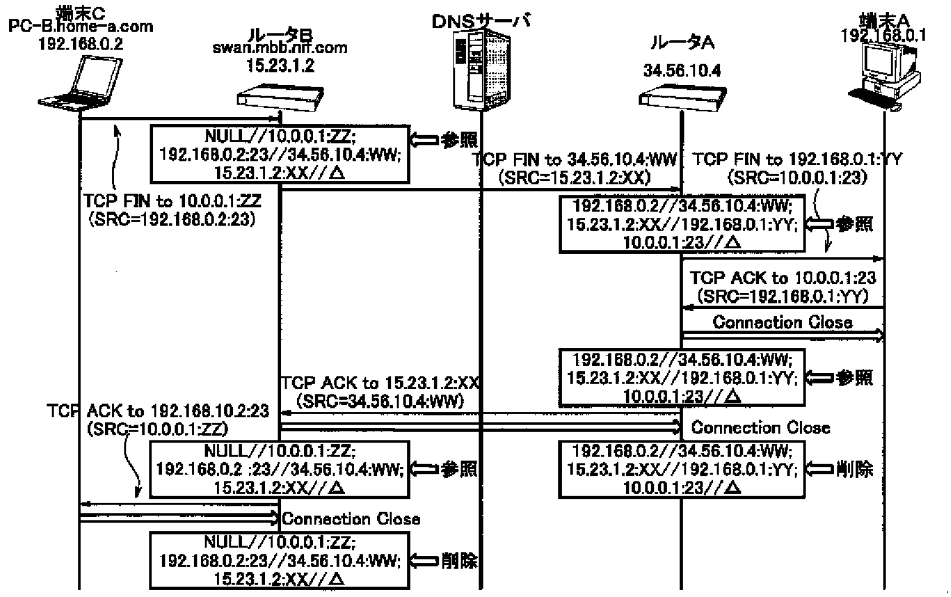
[Drawing 8]



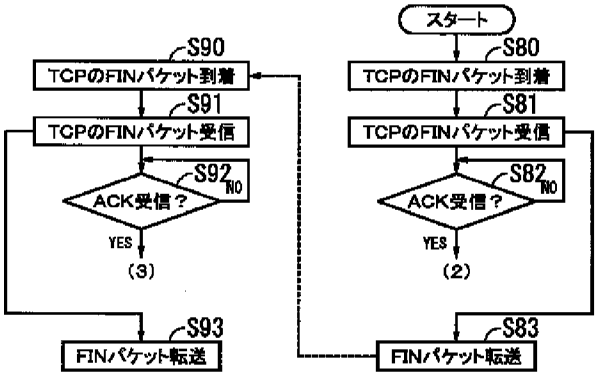
[Drawing 9]



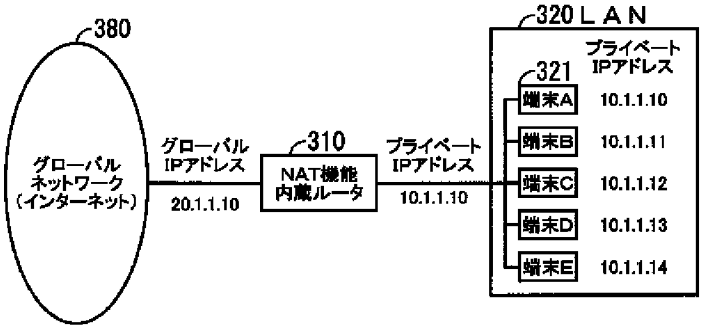
[Drawing 10]



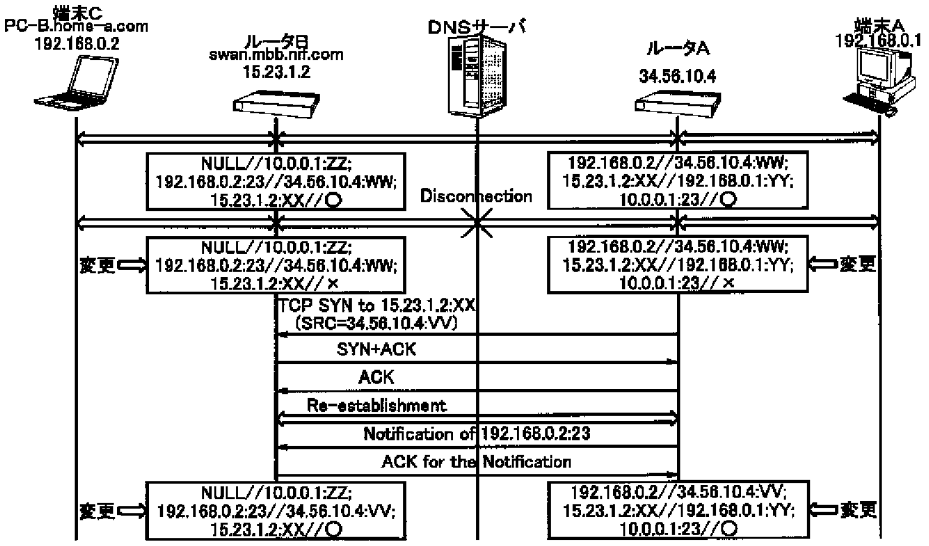
[Drawing 17]



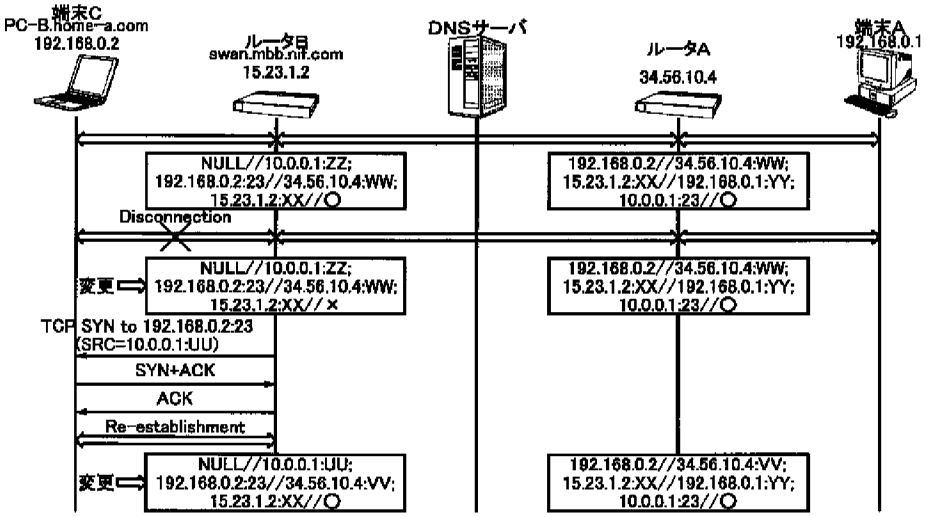
[Drawing 25]



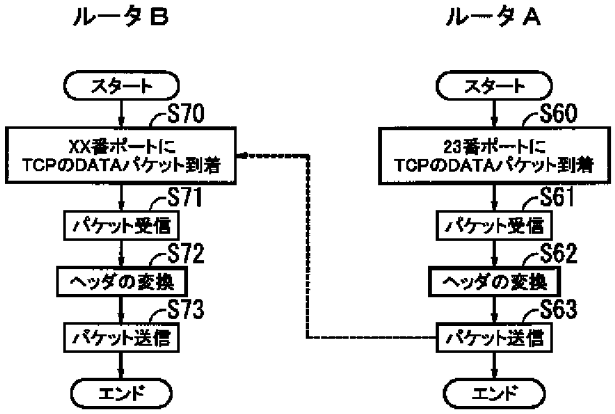
[Drawing 11]



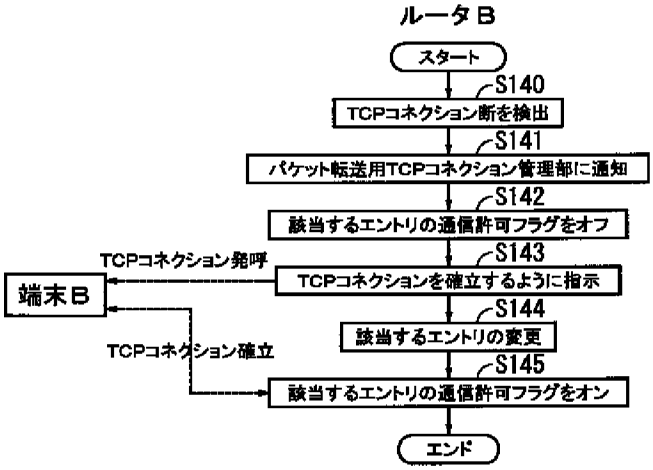
[Drawing 12]



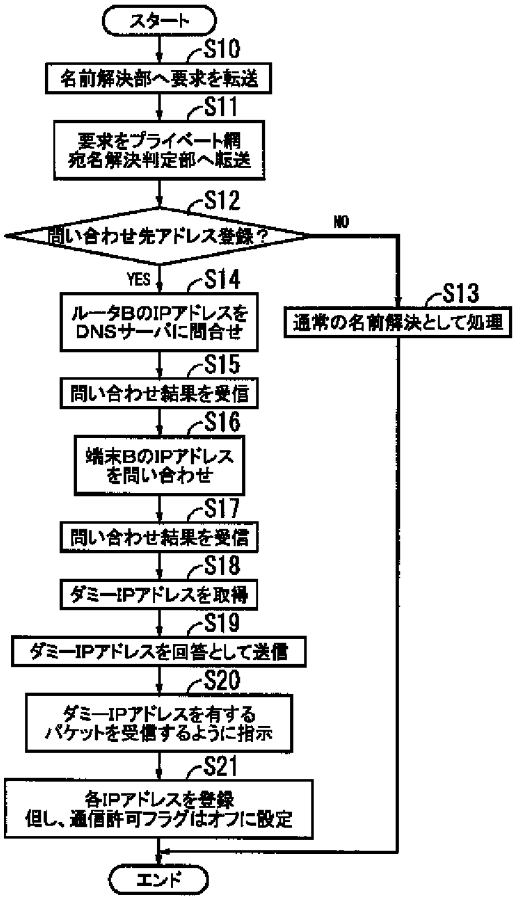
[Drawing 16]



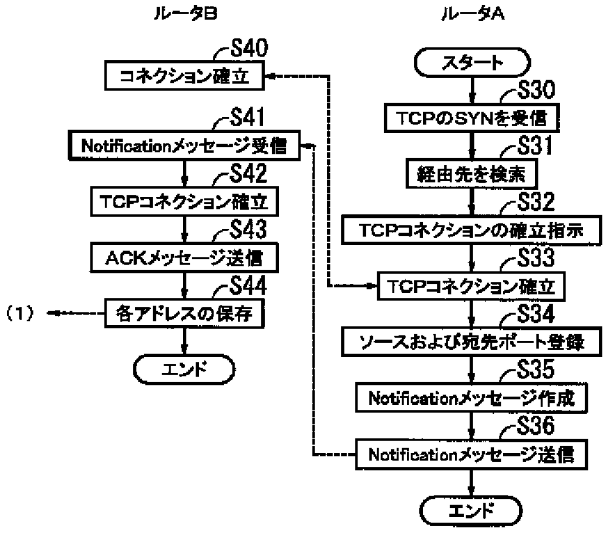
[Drawing 20]



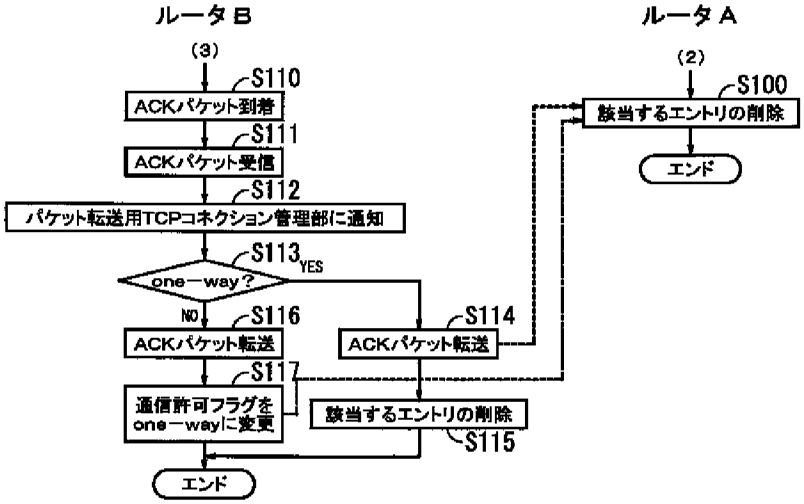
[Drawing 13]



[Drawing 14]



[Drawing 18]

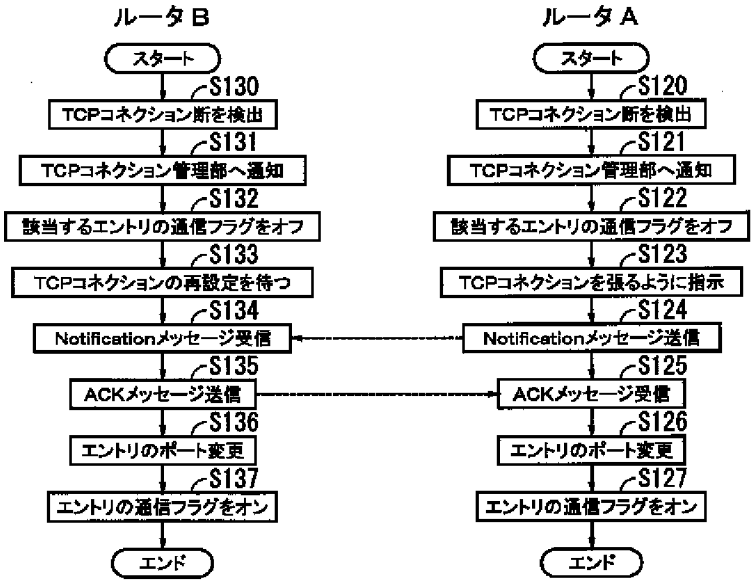


[Drawing 22]

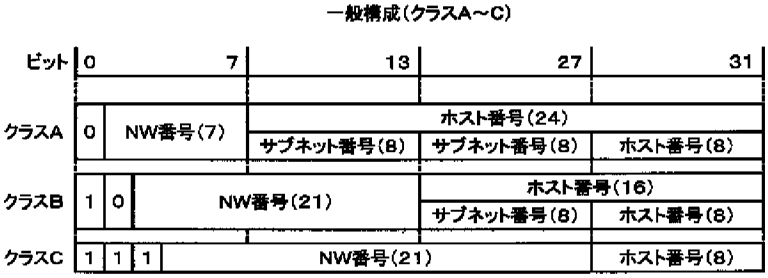
一般構成(クラスA～C)

ビット	0 7	13	27	31	IPアドレスの表現方法
クラスA	0～127	S/H(0～255)	S/H(0～255)	H(0～255)	10. H. H. H
クラスB	128～191	0～255	S/H(0～255)	H(0～255)	128. 20. H. H
クラスC	192～223	0～255	0～255	H(0～255)	192. 30. 100. H

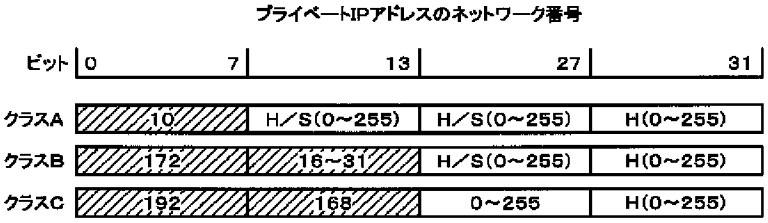
[Drawing 19]



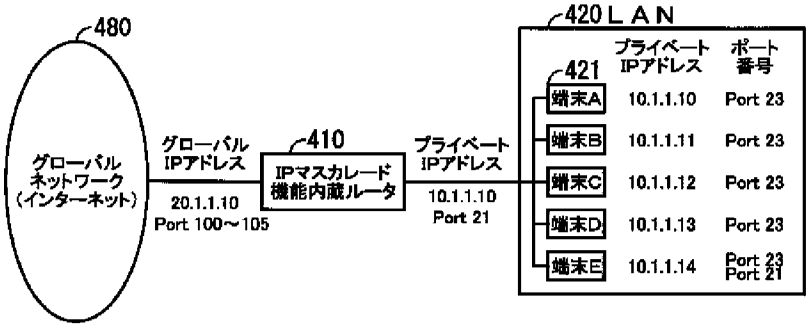
[Drawing 21]



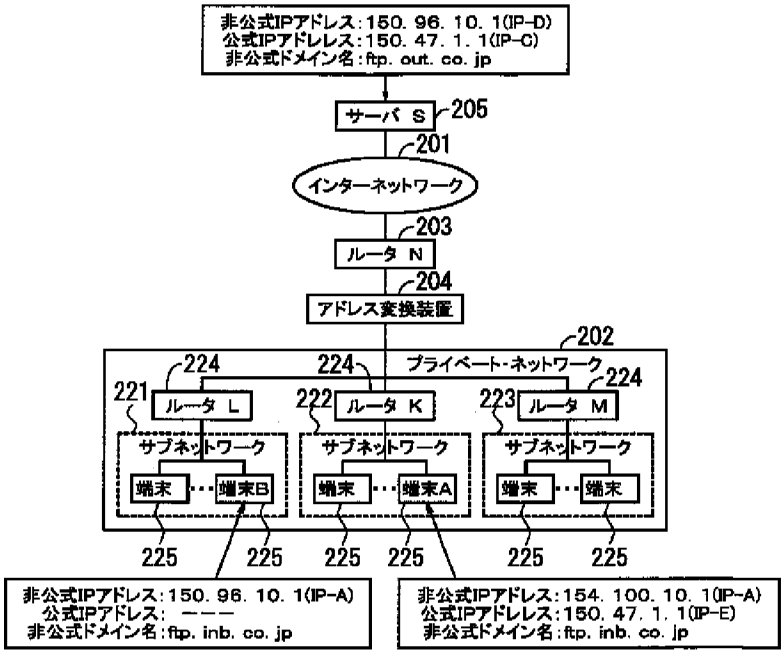
[Drawing 23]



[Drawing 26]



[Drawing 24]



[Drawing 27]

アプリケーション	グローバル・ネットワーク側（インターネット側）		プライベート・ネットワーク側（端末側）	
	IPアドレス	ポート番号	IPアドレス	ポート番号
Telnet	20.1.1.10	100	10.1.1.10	23
Telnet	20.1.1.10	101	10.1.1.11	23
Telnet	20.1.1.10	102	10.1.1.12	23
Telnet	20.1.1.10	103	10.1.1.13	23
Telnet	20.1.1.10	104	10.1.1.14	23
FTP	20.1.1.10	105	10.1.1.14	21

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－258838
（P2003－258838A）
(43)公開日　平成15年９月12日(2003.9.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ｂ	５Ｋ０３０
12/66		12/66	Ａ	

審査請求　未請求　請求項の数10　ＯＬ　（全 30 頁）

(21)出願番号　特願2002－58260(P2002－58260)

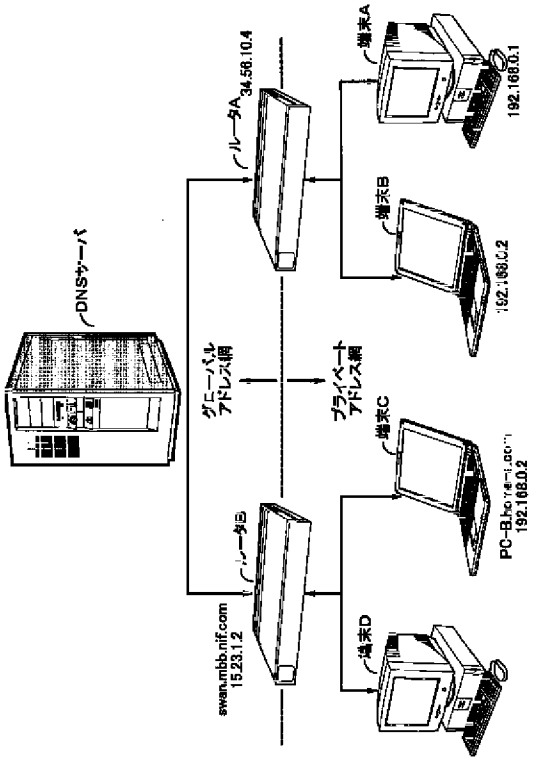
(22)出願日　平成14年３月５日(2002.3.5)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　小川　淳
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100092152
弁理士　服部　毅巖

Ｆターム(参考)　5K030 GA08 HA08 HB28 HC01 HD03

(54)【発明の名称】　通信装置およびネットワークシステム

(57)【要約】
【課題】　グローバルアドレス網からプライベートアドレス網へのアクセスを可能にする。
【解決手段】　アドレス変換装置は、プライベートアドレス網に属する各ノード（端末Ａ～Ｄ）に対して、ユニークな名前（ＦＱＤＮとしてのＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍ）を付与して管理し、グローバルアドレス網または他のプライベートアドレス網に属する所定のノードから所定の名前に対する問い合わせがなされた場合には、対応するプライベートアドレス（例えば、ＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍに対する問い合わせがなされた場合には１９２．１６８．０．２）を取得して通知する。また、グローバルアドレス網内のＤＮＳサーバのツリーには属さないプライベートアドレス網用のＤＮＳサーバはプライベートアドレス網毎に用意し、これをグローバルアドレス網からアクセスできるようにすることによりグローバルアドレス網経由でプライベートアドレスの名前解決を実現することができる。



【特許請求の範囲】
【請求項１】　第１のタイプのアドレスを有する通信装置で構成される第１のネットワークに属し、その配下に第２のタイプのアドレスを有する端末で構成される第２のネットワークを有する通信装置において、
他の通信装置の配下のネットワークに属する端末に付けられた名前を、当該他の通信装置に付けられた名前と対応して管理する手段と、
配下の端末から、通信相手となる端末に付けられた名前を受信した場合、前記管理手段により対応する通信装置に対してアドレス解決の要求を出力する手段と、
を設けたことを特徴とする通信装置。
【請求項２】　その配下の端末のアドレスをその端末に付けられた名前と対応させて管理する手段と、
前記他の通信装置からのその配下の端末のアドレス解決の要求に対して、前記管理手段によりアドレスを解決して、前記他の通信装置へ解決したアドレスを通知する手段と、
を設けたことを特徴とする請求項１記載の通信装置。
【請求項３】　アドレス解決の要求に対してアドレスの解決通知を前記他の通信装置から受信した場合、通知を受けたアドレスを前記第２のタイプのアドレスであって、その配下のネットワークの端末のアドレスとして用いられないアドレスに変換したダミーアドレスと対応づけて管理する手段と、
変換後の前記アドレスを通信を要求した端末へ通知する手段と、
を設けたことを特徴とする請求項２記載の通信装置。
【請求項４】　通信を要求した端末から、通知後のダミーアドレスを持つパケットを受信した場合、ダミーアドレスを前記他の通信装置のアドレスに変換する手段を設けたことを特徴とする請求項３記載の通信装置。
【請求項５】　第１のタイプのアドレスを有する通信装置で構成される第１のネットワークと、通信装置の配下で第２のタイプのアドレスを有する端末で構成される第２のネットワークとからなるネットワークシステムにおいて、
前記通信装置には、その配下の端末のアドレスをそれぞれの端末に付けられた名前と対応させて管理する第１の管理手段と、端末の名前をその端末のアドレスを管理する通信装置と対応させて管理する第２の管理手段と、を設け、
配下の端末からの通信要求に対して通信相手の端末のアドレスを解決する他の通信装置を前記第２の管理手段により求め、他の通信装置で前記第１の管理手段によりアドレス解決を行うことを特徴とするネットワークシステム。
【請求項６】　各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、これらの間でデータを伝送する際にアドレスの変換を行なうアドレス変換装置とを有するネットワークシステムにおいて、
前記アドレス変換装置は、前記プライベートアドレス網に属する各ノードに対して、ユニークな名前を付与して管理し、前記グローバルアドレス網または他のプライベートアドレス網に属する所定のノードから所定の名前に対する問い合わせがなされた場合には、対応するプライベートアドレスを取得して通知する、ことを特徴とするネットワークシステム。
【請求項７】　各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、前記グローバルアドレス網におけるアドレス変換を行なう第１のアドレス変換装置と、前記グローバルアドレス網と前記プライベートアドレス網との間におけるアドレス変換を行なう第２のアドレス変換装置とを有するネットワークシステムにおいて、
前記第１および第２のアドレス変換装置は、それぞれ独立にコネクションを確立し、相互にコネクションに関する情報を交換することにより、前記グローバルアドレス網と、前記プライベートネットワーク網との間で、データの授受を可能とする、ことを特徴とするネットワークシステム。
【請求項８】　前記第１のアドレス変換装置は、送信端末がコネクションを確立する際に、前記コネクションに関する情報を前記第２のアドレス変換装置に通知することを特徴とする請求項７記載のネットワークシステム。
【請求項９】　前記第１のアドレス変換装置は、受信端末の実際のプライベートアドレスとは異なるダミーのアドレスを送信端末に対して通知することを特徴とする請求項８記載のネットワークシステム。
【請求項１０】　前記ダミーのアドレスは、前記受信端末の実際のプライベートアドレスとはネットワーククラスが異なるアドレスであることを特徴とする請求項９記載のネットワークシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は通信装置およびネットワークシステムに関し、特に、各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、これらの間でデータを伝送する際にアドレスの変換を行なうアドレス変換装置とを有する通信装置およびネットワークシステムに関する。
【０００２】
【従来の技術】インターネット通信に使用されるＩＰアドレスは国際的に管理されており、インターネット通信を行なう場合にはＩＰアドレスを一元的に管理している国際的機関またはそれより委嘱を受けた管理機関（日本の場合、日本ネットワーク・インフォーメーション・セ

ンタＪＰＮＩＣまたはその代行者として承認されているプロバイダ）からインターネットにおいてユニークとなるＩＰアドレス（公式ＩＰアドレスとも呼ばれるが、以下、グローバルＩＰアドレスと記す）やドメイン名の配付を受けることになっている。従って、グローバルＩＰアドレスを取得しなければインターネット通信を行なうことはできず、また、通信を行ってはいけないことになっている。

【０００３】これに対して、インターネット通信を行なわないＬＡＮ（ローカルエリアネットワーク）などのネットワークでは任意のＩＰアドレス（以下、グローバルＩＰアドレス以外のＩＰアドレスを非公式ＩＰアドレスと記す）を使用することができる。しかし、インターネット技術の標準化組織であるＩＥＴＦ（International Engineering Task Force）が公開しているＲＦＣ（Request For Comments）においては、非公式ＩＰアドレスを使用している端末が間違ってインターネット接続を行った場合に問題が生じないよう、インターネット接続を行なわないＬＡＮなどではグローバルＩＰアドレスでないことが識別できる特定の番号をもつＩＰアドレス（非公式アドレスの一種であるが、以下、プライベートＩＰアドレスと記す）を使用することが推奨されている（詳細は後述）。

【０００４】一方、近年におけるインターネット通信の急速な増加に伴い、グローバルＩＰアドレスの枯渇が懸念される状況になっているため、大量のＩＰアドレスを必要とする企業や自治体などのネットワークに対してグローバルＩＰアドレスが充分に分配できない事態が生じている。このようなグローバルＩＰアドレスの不足に対処するため、企業などにおいてはＬＡＮの内部ではプライベートＩＰアドレス（または、非公式ＩＰアドレス）を使用し、外部のネットワークとインターネット通信を行なう場合にグローバルＩＰアドレスを用いる方法が一般的になりつつある。

【０００５】ところが、ＬＡＮ（プライベートネットワーク）の急速な増加とインターネット通信の普及に伴って、ＬＡＮ内での接続のみを想定してプライベートＩＰアドレスを用いて構築されたＬＡＮを、同じようにプライベートＩＰアドレスを用いて構築された他のネットワークと接続したい、というケースが増えつつある。この場合、次のような問題がある。前述のプライベートＩＰアドレスはアドレスの一部であるネットワーク番号部分が特定の数字に固定されており、プライベートＩＰアドレスとして使用できる番号の範囲が比較的狭いため、異なるネットワークで同一のプライベートＩＰアドレスが使用されている可能性が大きい。同一のプライベートＩＰアドレスが使用されている可能性があるネットワーク同士をグローバルなインターネットを介さずに直接接続する場合、個々の端末に付与されているプライベートＩＰアドレスや、アドレスに関与するサーバなどの設定内容を変更しないことが望ましい。このような状況から、プライベートＩＰアドレスを独自に使用している別個のネットワーク相互を、既に稼働されている各ネットワークの環境を変更することなしに接続できるようにするＩＰアドレス変換装置の実現が望まれている。

（１）ＩＰアドレスの構成

周知のように、ＴＣＰ／ＩＰプロトコルを使用するインターネット通信におけるＩＰアドレスはネットワークを識別するためのアドレス部分（以下、ネットワーク番号と記す）と、そのネットワーク内の個々のホスト（端末）を識別するためのアドレス部分（以下、ホスト番号と記す）からなる３２ビットで構成されている。しかし、企業のネットワークには、内部のホスト数が多い大規模なネットワークがある一方で、個々のネットワーク（ローカル網）のホスト数は少ないが多数のネットワーク（ローカル網）を広範囲の地域に持つものも多いため、ネットワーク番号の桁数はネットワークの規模・構成によって変えている。「クラス」はネットワーク番号に何桁を使用するネットワークであるか示すものである。

【０００６】図２１は各クラスのＩＰアドレスの構成を図示したものであるが、図示のように、クラスＡは先頭のビットが“０”で、続く７ビットがネットワーク番号（他の図面を含め、図ではネットワーク番号をＮＷ番号とも記す）で、残り２４ビットがホスト番号となっている。図２１の括弧内はネットワーク番号とホスト番号に使用されるビット数である。また、クラスＢは先頭の２ビットが２進数で“１０”、続く２１ビットがネットワーク番号、クラスＣは先頭の３ビットが２進数で“１１１”、続く２１ビットがネットワーク番号になっている。このほかにクラスＤなどもあるが図示は省略する。

【０００７】図２１に示すように、クラスＡでは２４ビットをホスト番号に使用できるが、実際にはネットワーク内の端末に随意にホスト番号を割り付けることは少なく、ネットワーク内を更に階層化するのが普通である。階層化されたネットワークをサブネットワーク（以下、「サブネット」と記す）と呼び、各サブネットに付与したＩＰアドレスの部分をサブネット番号と呼んでいる。サブネット番号はホスト番号の一部を使用するもので、ホスト番号との関係を図２１に示す。サブネットの数及び個々のサブネットに付与するサブネット番号のビット数は随意であるが、サブネット番号は図２１に記載したように８ビットを単位として割り付けるのが最も一般的である。

【０００８】３２ビットのＩＰアドレスは慣習的に８ビットずつ区切って４つの１０進数で表示するようになっている（以下、４つの１０進数の各々、即ち、８ビット単位の数を「桁」と記す）が、クラスを示すビットの数値は最初の８ビット中のネットワーク番号と合わせて１０進数で表示する。この表示方法によれば、各クラスの

ＩＰアドレスに使用される数字の範囲は図２２に記すような値になり、クラスＡでは最初のビットが“０”であるため、最初の桁は１０進数で「０～１２７」(実際に使用できるのは「０～１２６」)の範囲となる（以下、各桁の数値は特に断らない限り１０進数で記す）。

【０００９】クラスＢは最初の２ビットが２進数で“１０”であるので、最初の桁の数値範囲は「１２８～１９１」となる。クラスＣも同様であるが、説明を省略したクラスＤ（最初の４ビットが２進数で“１１１０”）やクラスＥ（最初の５ビットが２進数で“１１１１０”）があるため、最初の桁に使用できる数値の範囲は「１９２～２５５」でなく「１９２～２２３」になる。また、最初の桁以外の３つの桁のネットワーク番号またはホスト番号（サブネット番号）に使用できる数値の範囲は「０～２５５」になる。そして、各クラスのＩＰアドレスは図２２の右側に記載したように１０進数で、「１０．Ｈ．Ｈ．Ｈ」（クラスＡの例）のように表現される（Ｈはホスト番号で、実際には０～２５５の数字で表される）。従って、最初の桁の数値によってＩＰアドレスのクラスを識別することができる。

【００１０】以上のＩＰアドレスの構成はグローバルＩＰアドレスでもプライベートＩＰアドレスでも同一であるが、前記ＩＥＴＦが公開しているＲＦＣ１５９７ではグローバルＩＰアドレスでないことが識別できるプライベートＩＰアドレスの使用を推奨している。図２３はＲＦＣ１５９７に規定されているプライベートＩＰアドレスの数値を示したものであるが、図示のように、プライベートＩＰアドレスについては斜線を施した部分について使用できる数値範囲が定められている。例えば、クラスＡのプライベートＩＰアドレスは最初の８桁が“１０”（１０進数）に限定され、クラスＢとクラスＣでは最初の桁と次の桁について使用する数字が限定されている。クラスＣの場合には最初の２桁がそれぞれ一つの数値に限定されているため任意に使用できるネットワーク番号とホスト番号の数はそれぞれ２５６しかない。

【００１１】異なるネットワークで全く同一のアドレスが使用される確率はネットワーク内のホスト数などが大きく影響するのでどのクラスが高いとは言えないが、どのクラスも３２ビット中に自由に使用できない数値が存在する分、選択範囲が狭くなるので、プライベートＩＰアドレスにおいては異なるネットワークで同一アドレスが使用される確率は高くなる。従って、独自にプライベートＩＰアドレスを割り付けた２つのネットワークで通信を行なう場合には、両ネットワークに同一アドレスが存在することを前提とする必要がある。

（２）プライベートＩＰアドレス使用端末のインターネット接続方法

次に、プライベートＩＰアドレスを使用している２つのネットワークにそれぞれ属する端末間を接続する従来技術について説明する。従来技術ではプライベートＩＰアドレスを使用しているネットワークが他のネットワークと通信を行なう場合にグローバルなインターネットを介して接続する方法がとられている。この方法は、特開平９－２３３１１２号公報などにも記載されているが、以下、同公報に記載されている一方の端末がグローバルＩＰアドレスをもつ端末（サーバを含む）である場合を例に、従来技術の接続方法を説明する。

【００１２】図２４は前記公報中の図１に記載されているインターネットワーク環境のブロック図に同公報の説明内容を要約して付加したものである。同公報中の「公式ＩＰアドレス」は本明細書中に記載されている「グローバルＩＰアドレス」と同一のものであるが、図２４の説明の中では同公報の記載に合わせて公式ＩＰアドレスと記す。また、同公報記載の「非公式ＩＰアドレス」は本明細書中の「非公式ＩＰアドレス」（プライベートＩＰアドレスよりも範囲が広い）と同一のものであるのでそのまま使用する。

【００１３】いま、図２４のプライベートネットワーク２０２内の端末２２５（個々の端末を指す場合は端末Ａなどと記す）には何れも非公式ＩＰアドレスのみが付与されているが、その中の端末Ａがプライベートネットワーク２０２外のサーバ２０５（以下、サーバＳと記す）に対して接続を行なうものとする。

【００１４】送信元の端末Ａは送信相手のドメイン名は知っているので、サーバＳのドメイン名（「ftp.out.co.jp」とする）からそのＩＰアドレスを問い合わせる。端末Ａが接続されているルータ２２４（以下、ルータＫと記す）はインターネットワーク２０１側に設けられたルータ２０３（以下、ルータＮと記す）を介し、周知の方法でこのドメイン名をもつ端末（サーバなどを含む）のＩＰアドレスをインターネットワーク２０１側に問い合わせる。その結果、前記ドメイン名をもつサーバＳの公式ＩＰアドレス（「１５０．９６．１０．１」とし、「ＩＰ－Ｄ」と略記する）がインターネットワーク２０１側から回答される。

【００１５】ここでアドレス変換装置２０４がないものとし、ルータＮがルータＫを介し端末Ａにこの公式ＩＰアドレス「１５０．９６．１０．１」を通知したとすると、端末Ａは以後、送信するパケットのヘッダ内の送信先アドレスにこのＩＰアドレスを設定して送信することになる。ところが、図の例ではプライベートネットワーク２０２内の端末ＢがＩＰ－Ｄと全く同一番号の非公式ＩＰアドレスをもっているので、端末Ａが「１５０．９６．１０．１」を送信先アドレスに設定した場合にはパケットが端末Ｂに送信される可能性がある。

【００１６】このような事態を生じさせないために、図２４ではプライベートネットワーク２０２とルータＮの間に設けられたアドレス変換装置２０４においてアドレスの変換を行なう。アドレス変換装置２０４は、端末Ａからサーバ Ｓのドメイン名を送信先アドレスとするＩＰ

パケットを受信すると、サーバＳのＩＰアドレスをインターネットワーク２０１側に問い合わせるとともに、サーバＳの非公式アドレスとしてプライベートネットワーク２０２内のみ有効であり、かつ、プライベートネットワーク２０２内で現在使用されていない非公式ＩＰアドレス（「１５９．９９．３０．１」とし、「ＩＰ－Ｃ」と略記する）を選定して端末Ａに通知する。以後、端末Ａは送信先のＩＰアドレスに非公式ＩＰアドレスの「ＩＰ－Ｃ」を設定してパケットを送信する。

【００１７】次いで、先の問合せに対してインターネットワーク２０１側からサーバＳの公式ＩＰアドレス「１５０．９６．１０．１」が回答されると、アドレス変換装置２０４は公式ＩＰアドレス「ＩＰ－Ｄ」と非公式ＩＰアドレス「ＩＰ－Ｃ」を対応させて記憶しておき、端末Ａから送信されるパケットの送信先アドレスの「ＩＰ－Ｃ」を「ＩＰ－Ｄ」に変換してインターネットワーク２０１側に送出する。

【００１８】一方、端末Ａには非公式ＩＰアドレス（「１５４．１００．１０．１」とし、「ＩＰ－Ａ」と略記する）が付与されているので、パケットの送信元のアドレスにはこの「ＩＰ－Ａ」を設定する。インターネットワーク２０１には非公式ＩＰアドレスは通用しないため、アドレス変換装置２０４は周知の方法で端末Ａに対して公式ＩＰアドレス（「１５０．４７．１．１」とし、「ＩＰ－Ｅ」と略記する）を取得し、「ＩＰ－Ａ」と「ＩＰ－Ｅ」の対応を記憶しておく。以後、端末Ａから送信されるパケットの送信元ＩＰアドレスに設定されている「ＩＰ－Ａ」は「ＩＰ－Ｅ」に変換して送信する。

【００１９】サーバＳ側から端末Ａにパケットを送信する場合には送信先ＩＰアドレスとして端末Ａの公式ＩＰアドレス「ＩＰ－Ｅ」を設定するが、アドレス変換装置２０４はサーバＳから受信したパケットの送信先アドレス「ＩＰ－Ｅ」を「ＩＰ－Ａ」に変換してプライベートネットワーク２０２に送信する。従って、プライベートネットワーク２０２内に送信先の公式ＩＰアドレス「ＩＰ－Ｅ」と同一番号の非公式ＩＰアドレスをもつ端末２２５が存在してもその端末に対してパケットが送信されることはない。

（３）ＩＰアドレス変換方法

以上、プライベートＩＰアドレスを使用するネットワーク（プライベートネットワーク）内の端末がインターネット接続を行なう際における従来のアドレス変換技術を接続手順を主体に説明したが、次に、従来技術におけるアドレスの変換方法について説明する。

【００２０】上記の例ではアドレス変換装置を設けてアドレス変換を行っているが、従来技術では、ＮＡＴやＩＰマスカレード（または、マルチＮＡＴ）と呼ばれる技術をルータ或いはファイアウォールサーバに内蔵させることによりアドレスの変換を行なう方法が一般的に知られている。

【００２１】ＮＡＴ：最初にＮＡＴ（Network Address Translation ）について説明する。ＮＡＴはＲＦＣ１６３１で規定されているアドレス変換方式で、プライベートＩＰアドレスとグローバルＩＰアドレスを変換する機能である。低価格のルータにはこのＮＡＴ機能の搭載を一つの特徴としているものも多い。図２５はＮＡＴ機能を説明する図で、ネットワークの構成とＩＰアドレスの使用形態のモデルを示している。図２５ではプライベートなネットワーク（以下、ＬＡＮと記す）３２０に接続されている複数の端末３２１（特定の端末を指す場合には端末Ａなどと記す）に各々には図中に記載したようなプライベートＩＰアドレスが付与されているものとする。

【００２２】このような構成において、ＬＡＮ３２０に接続されているプライベートＩＰアドレス「１０．１．１．１０」をもつ端末Ａからインターネット通信（具体的にはグローバル・ネットワーク３８０を介して図示省略された他のネットワーク内の端末に接続）を行なう場合には、端末Ａはルータ３１０を介してインターネット側で使用するグローバルＩＰアドレスとして、例えば、「２０．１．１．１０」を取得する。

【００２３】ルータ３１０はＮＡＴ機能を内蔵しているが、端末Ａはルータ３１０内のＮＡＴ機能により、インターネット側に対してはプライベートＩＰアドレスの「１０．１．１．１０」がグローバルＩＰアドレスの「２０．１．１．１０」に変換され、インターネット側から送られてくる送信先アドレスのグローバルＩＰアドレス「２０．１．１．１０」をもつパケットはＮＡＴ機能により送信先がプライベートＩＰアドレスの「１０．１．１．１０」に変換されて端末Ａに送られる。従って、この例ではグローバルＩＰアドレスの「２０．１．１．１０」とプライベートＩＰアドレスの「１０．１．１．１０」が対応して使用されている形になる。図２４により説明したＩＰアドレスの変換方法はＮＡＴを利用した方法であるとみることもできる。

【００２４】このように接続時にグローバルＩＰアドレスを付与してインターネット接続を行なわせる方法は端末型ダイヤルアップＩＰ接続サービスなどと呼ばれているが、この方法では接続を行なう端末のみがグローバルＩＰアドレスを使用するので、一つのグローバルＩＰアドレスをＬＡＮ内の複数の端末３２１で共通に使用することができる。しかし、一つのＬＡＮ３２０が同時に使用できるグローバルＩＰアドレスの数は予めＪＰＮＩＣまたはその代行者（プロバイダなど）との契約によって定まっているため、その数以上の端末が同時にインターネット接続を行なうことはできない。また、グローバルＩＰアドレスは複数の端末２２１が共用するため、インターネット側から送信先アドレスにグローバルＩＰアドレス（例えば、「２０．１．１．１０」）を設定してＬ

ＡＮ３２０内の特定の端末を指定することはできない。

【００２５】ＩＰマスカレード（マルチＮＡＴ）：次に、ＩＰマスカレード（マルチＮＡＴとも呼ばれる）について説明する。ＩＰマスカレードもＮＡＴに似ているが、ＮＡＴがプライベートＩＰアドレスとグローバルＩＰアドレスの変換、即ち、ＩＰアドレス部分のみを変換するのに対して、ＩＰマスカレードはポート番号も利用してアドレス変換を行なう。周知のように、ＩＰアドレスはＯＳＩ参照モデルにおける第３層に位置し、送信先アドレス及び送信元アドレスはＲＦＣ７９１で規定されるＩＰヘッダ内に設定される。これに対して、ポートはＯＳＩ参照モデルの最上位に当たる第５層のアプリケーション対応に付与され、ポート番号はＩＰ層（第３層）の上位に当たる第４層に位置するＴＣＰプロトコルにより設定される。従って、ポート番号はＩＰヘッダ内には設定されない。ポート番号の割り当てはローカルにそれぞれのホスト（端末）で行われるが、予め知っていないと最初の処理ができないというようなアプリケーションサービスに使用されるポート番号については特定のポート番号が固定的に定められている。

【００２６】図２６および図２７はＩＰマスカレードを説明する図で、図２６はネットワークの構成とＩＰアドレスの使用形態のモデルを示し、図２７はプライベートＩＰアドレスとグローバルＩＰアドレスの対応の一例を示している。図２６の例ではプライベートなネットワーク（ＬＡＮと記す）４２０に接続されている複数の端末４２１（特定の端末を指す場合には端末Ａなどと記す）の各々に図中に記載したようなプライベートＩＰアドレスが付与されている。また、同図には各端末４２１で使用されるアプリケーションの一部に使用されているポート番号が記載されている。ポート番号はアプリケーション対応に付与されるので一つの端末に複数設定されるのが普通であるが、図にはアプリケーションの一種であるＴｅｌｎｅｔに固定的に割り当てられているポート番号“２３”が全端末４２１に使用され、端末ＥにはＦＴＰ（File Transfer Protocol）に固定的に割り当てられているポート番号“２１”が併用されている例が図示されている。

【００２７】ＩＰマスカレードでも一つ（または定められた数）のグローバルＩＰアドレスを複数の端末４２１が共用するが、グローバルＩＰアドレス側には端末が識別できるポート番号を設定する。例えば、端末Ａ～端末ＥにはインターネットＩＰアドレスとして「２０．１．１．１０」が割り当てられるほか、各端末４２１のプライベートＩＰアドレスとポート番号（アプリケーションの種類に対応）の組み合わせごとに個別のポート番号が割り当てられる。図２７にポート番号を含むプライベートＩＰアドレスとグローバルＩＰアドレスの対応の例を記す。この例では、アプリケーションとしてＴｅｌｎｅｔが使用される場合、インターネット側のポート番号として、端末Ａに“１００”、端末Ｂに“１０１”、以下同様にして端末Ｅに“１０４”が割り当てられている。端末Ｅのようにアプリケーションとしてもｆｔｐも使用される場合は例えばＴｅｌｎｅｔ（端末側のポート番号“２３”）に対してポート番号“１０４”、ＦＴＰ（端末側のポート番号“２１”）に対してポート番号“１０５”が割り当てられる。

【００２８】

【発明が解決しようとする課題】以上のように、従来技術であるＮＡＴやＩＰマスカレードでは、プライベートアドレスを有する端末からグローバルアドレスを有する端末へのアクセスという一方向通信のみが実現されている。グローバルアドレスを有する端末からプライベートアドレスを有する端末へのアクセスや、プライベートアドレスを有する二つの網間での通信は行なえなかった。これらの実現には、グローバルアドレスを新たに取得し、プライベートアドレスを有する端末へ割り当てる必要があり、手続きや費用を要するという問題点があった。

【００２９】また、ＮＡＴやＩＰマスカレードは下記の技術的制約により一方向通信サービスしか提供できないという問題点があった。

１．プライベートアドレス網同士はそれぞれ重複するアドレス空間を用いているため、プライベートアドレス網内の端末を一意化する手法がない。

２．現在のＤＮＳによる名前解決手法は、グローバルアドレス網からプライベートアドレス網内の端末のＩＰアドレスを取得する手段がない。

３．グローバルアドレス網のルータがプライベートアドレスの経路情報を扱う手法がない。即ち、プライベートアドレス網からグローバルアドレス網へのＩＰの経路がないためＴＣＰコネクションを張ることができない。

【００３０】本発明は以上の点に鑑みてなされたものであり、プライベートアドレスを有する端末への通信を実現する。

【００３１】

【課題を解決するための手段】本発明では上記課題を解決するために、第１のタイプのアドレスを有する通信装置で構成される第１のネットワークに属し、その配下に第２のタイプのアドレスを有する端末で構成される第２のネットワークを有する通信装置において、他の通信装置の配下のネットワークに属する端末に付けられた名前を、当該他の通信装置に付けられた名前と対応して管理する手段と、配下の端末から、通信相手となる端末に付けられた名前を受信した場合、前記管理手段により対応する通信装置に対してアドレス解決の要求を出力する手段と、を設けたことを特徴とする通信装置が提供される。

【００３２】ここで、第２のタイプのアドレスであるプ

ライベートアドレスを有する端末（ノード）に対してもユニークな名前である、例えば、ＦＱＤＮ（fully-qualified domain name：ホスト名，ドット，ドメイン名の三つで構成するホストの名前。www.fts.comなど）を割り当て、その端末を有する他の通信装置に付けられた第１のタイプのアドレスであるグローバルアドレスと対応づけて管理し、配下の端末から通信相手となる端末に付けられたプライベートアドレスを受信した場合には、対応する他の通信装置を特定し、特定された他の通信装置に対してアドレスの解決要求を行うことにより、プライベートアドレス網、グローバルアドレス網を問わず、ユニークな識別子を端末に付与することができる。

【００３３】また、本発明では上記課題を解決するために、第１のタイプのアドレスを有する通信装置で構成される第１のネットワークと、通信装置の配下で第２のタイプのアドレスを有する端末で構成される第２のネットワークとからなるネットワークシステムにおいて、前記通信装置には、その配下の端末のアドレスをそれぞれの端末に付けられた名前と対応させて管理する第１の管理手段と、端末の名前をその端末のアドレスを管理する通信装置と対応させて管理する第２の管理手段と、を設け、配下の端末からの通信要求に対して通信相手の端末のアドレスを解決する他の通信装置を前記第２の管理手段により求め、他の通信装置で前記第１の管理手段によりアドレス解決を行うことを特徴とするネットワークシステムが提供される。

【００３４】ここで、通信装置の第１の管理手段は、配下の端末に付けられた第２のアドレスであるプライベートアドレスとユニークな名前である、例えば、ＦＱＤＮとを対応づけて管理し、第２の管理手段は、端末の名前（ＦＱＤＮ）と、その端末を管理する通信装置の第１のアドレスであるグローバルアドレスとを対応づけて管理し、配下の端末から通信要求がなされた場合には、第２の管理手段によってアドレス解決を行う通信装置を特定し、他の通信装置の第１の管理手段によってアドレス解決を行うようにしたので、グローバルアドレス網経由でプライベートアドレスの名前解決を実現することができる。

【００３５】更に、本発明では上記課題を解決するために、各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、これらの間でデータを伝送する際にアドレスの変換を行なうアドレス変換装置とを有するネットワークシステムにおいて、前記アドレス変換装置は、前記プライベートアドレス網に属する各ノードに対して、ユニークな名前を付与して管理し、前記グローバルアドレス網または他のプライベートアドレス網に属する所定のノードから所定の名前に対する問い合わせがなされた場合には、対応するプライベートアドレスを取得して通知する、ことを特徴とするネットワークシステムが提供される。

【００３６】ここで、プライベートアドレス網に属するノードに対してもユニークな名前である、例えば、ＦＱＤＮを割り当てることにより、プライベートアドレス網、グローバルアドレス網を問わず、ユニークな識別子を端末が有することができる。また、グローバルアドレス網内のＤＮＳサーバのツリーには属さないプライベートアドレス網用のＤＮＳサーバはプライベートアドレス網毎に用意し、これをグローバルアドレス網からアクセスできるようにすることによりグローバルアドレス網経由でプライベートアドレスの名前解決を実現することができる。

【００３７】また、本発明では上記課題を解決するために、各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、前記グローバルアドレス網におけるアドレス変換を行なう第１のアドレス変換装置と、前記グローバルアドレス網と前記プライベートアドレス網との間におけるアドレス変換を行なう第２のアドレス変換装置とを有するネットワークシステムにおいて、前記第１および第２のアドレス変換装置は、それぞれ独立にコネクションを確立し、相互にコネクションに関する情報を交換することにより、前記グローバルアドレス網と、前記プライベートネットワーク網との間で、データの授受を可能とする、ことを特徴とするネットワークシステムが提供される。

【００３８】ここで、プライベートアドレス網内でのコネクションとグローバルアドレス網内でのコネクションを第１および第２のアドレス変換装置が別個に確立し、第１および第２のアドレス変換装置が両コネクションに関する情報を交換（マップ）することで、グローバルアドレス網からプライベートアドレス網へのＴＣＰコネクションを実現することが可能になる。

【００３９】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。なお、通信装置は、ノードをいい、例えば、ルータである。第１のタイプのアドレスとは、例えば、グローバルアドレスであり、第２のアドレスとは、例えば、プライベートアドレスである。

【００４０】図１は、本発明の実施の形態の構成例を示す図である。この図に示すように、本発明の実施の形態は、端末Ａ～Ｄ、ルータＡ，Ｂ、ＤＮＳサーバによって構成されている。

【００４１】ここで、端末Ａ，Ｂは、ルータＡを介して相互に接続されており、プライベートアドレス網を構成している。なお、端末Ａには、プライベートアドレスとして１９２．１６８．０．１が付与されている、一方、端末Ｂには、プライベートアドレスとして１９２．１６８．０．２が付与されている。

【００４２】ルータＡは、端末Ａ，Ｂ間でパケットを転

送するとともに、グローバルアドレス網を介してパケットを転送する場合には、アドレス変換を実行する。なお、ルータAには、グローバルアドレスである、３４．５６．１０．４が付与されている。

【００４３】ＤＮＳサーバは、そのサーバの管理下にある、各ノードのＩＰアドレスと、名前（ホスト名）の対応を記録したデータベースを保持しており、各ノードからの問い合わせに応じてデータベースを検索して、その結果を返す。また、自分の管理下にないドメインのホストの検索の場合は、さらに上位のＤＮＳサーバ（図示せず）に対して代理で問い合わせを行ない、その結果を返す。

【００４４】ルータBは、端末C，D間でパケットを転送するとともに、グローバルアドレス網を介してパケットを転送する場合には、アドレス変換を実行する。なお、ルータBには、グローバルアドレスである１５．２３．１．２およびホスト名であるｓｗａｎ．ｍｂｂ．ｎｉｆ．ｃｏｍが付与されている。

【００４５】端末C，Dは、ルータBを介して相互に接続されており、プライベートアドレス網を構成している。なお、端末Cには、プライベートアドレスとして１９２．１６８．０．２およびホスト名としてＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍが付与されている。なお、ホスト名としてはＦＱＤＮを採用する。

【００４６】図2は、ルータAおよびルータBの詳細な構成例を示す図である。この図に示すように、ルータA，Bは、ＩＰ部１０、ＴＣＰ部１１、名前解決部１２、プライベート網宛名前解決判定部１３、通信先プライベート網用名前解決サーバ登録部１４、ダミーＩＰアドレスプール部１５、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６、パケット転送部１７、パケット転送用ＴＣＰコネクション管理部１８、および、通信先端末アドレス／ポートネゴシエーション部１９によって構成され、その外部には通信手段２０およびコンソール２１が接続されている。

【００４７】ここで、ＩＰ部１０は、２つのノード間でＴＣＰのパケットを送受信する役目を担っている。即ち、ＩＰアドレスによって識別される２つのノード間においてＴＣＰパケットを配送する。なお、ＩＰ部１０は、受信を許可されているＩＰアドレスの一覧を保持する受信許可ＩＰアドレス保持部１０ａを有している。

【００４８】ＴＣＰ部１１は、２つのアプリケーション間で、通信を行なうためのプロトコルであるコネクションを確立する。即ち、まず最初に、アプリケーション間でコネクションを確立し、そのコネクションを使用して双方向の通信を実現する。なお、ＴＣＰ部１１は、受信ポートを変更するための受信ポート変更部１１ａを有している。

【００４９】名前解決部１２は、ＤＮＳによる名前解決要求がなされた場合には、名前解決処理を実行する。プライベート網宛名前解決判定部１３は、通信先プライベート網用名前解決サーバ登録部１４へ問合せ先アドレスのエントリの有無をチェックするとともに、名前解決処理を実行する。

【００５０】通信先プライベート網用名前解決サーバ登録部１４は、プライベート網用の名前解決サーバに関する情報を格納している。ダミーＩＰアドレスプール部１５は、プライベート網に属するノードと通信する際に使用するダミーＩＰアドレスを一定数保持している。

【００５１】通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６は、受信端末と送信端末の間でデータを授受する際に必要な各ノードのＩＰアドレスおよびダミーＩＰアドレスをエントリとして登録する。

【００５２】パケット転送部１７は、パケットを転送する際に必要な処理を実行する。パケット転送用ＴＣＰコネクション管理部１８は、パケット転送部１７の指示に従ってコネクションを確立する。

【００５３】通信先端末アドレス／ポートネゴシエーション部１９は、ＮｏｔｉｆｉｃａｔｉｏｎメッセージおよびＡＣＫメッセージを生成して送信する。通信手段２０は、伝送路を含む物理層であり、ＩＰ部１０から供給されたパケットを対応する電気信号に変換して送信するとともに、他のノードから送信されてきたパケットを対応する電気信号に変換してＩＰ部１０に供給する。

【００５４】コンソール２１は、通信先プライベート網用名前解決サーバ登録部１４に対して情報を登録する際のインタフェースである。次に、以上の実施の形態の動作について説明する。

【００５５】先ず、図3を参照して、プライベート網に属する端末Aが同じくプライベート網に属する端末Cに対してアクセスする際の名前解決処理について説明する。最初に、ルータAの通信先プライベート網用名前解決サーバ登録部１４に対して、図3に示すようなデータをコンソール２１を介して登録する。即ち、通信先プライベート網用名前解決サーバ登録部１４には、図3に示すような情報「＊．ｈｏｍｅ－ａ．ｃｏｍ／／ｓｗａｎ.ｍｂｂ．ｎｉｆ．ｃｏｍ」が登録される。この情報は、図4に示すように、解決要求された名前と、解決問い合わせ先の名前解決サーバの組み合わせからなる情報であり、いまの例では、＊．ｈｏｍｅ－ａ．ｃｏｍが解決要求された名前であり、また、ｓｗａｎ.ｍｂｂ．ｎｉｆ．ｃｏｍが解決問い合わせ先の名前解決サーバの名前である。なお、「＊」はワイルドカードを示し、任意の文字または文字列を意味する。

【００５６】次に、端末Aが端末Cのホスト名であるＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍに対する問い合わせを行なうために、ルータAに対してＤＮＳ　ｑｕｅｒｙを送信すると（図3参照）、ルータAは通信手段２０、ＩＰ部１０、および、ＴＣＰ部１１を介してこのデータを受信し、名前解決用送受信ポートを介して名前解決部１２

に供給する。

【００５７】名前解決部１２は、このような要求をプライベート網宛名前解決判定部１３へ転送する。プライベート網宛名前解決判定部１３は、通信先プライベート網用名前解決サーバ登録部１４のエントリを検索し、この要求に対応するエントリの有無を確認し、エントリが存在する場合にはそのエントリに関する情報を名前解決部１２に対して通知する。また、エントリが存在しない場合には、通常の名前解決を実行するように名前解決部１２に指示する。

【００５８】名前解決部１２は、通常の名前解決を実行するように指示された場合には、通常の名前解決処理を実行する。それ以外の場合には、エントリに関する情報を参照し、解決問い合わせ先の名前解決サーバを特定する。いまの例では、解決問い合わせ先の名前解決サーバのホスト名は「ｓｗａｎ．ｍｂｂ．ｎｉｆ．ｃｏｍ」であり、これは、ルータＢに対応しているので、名前解決部１２は、図３に示すように、先ず、ホスト名「ｓｗａｎ．ｍｂｂ．ｎｉｆ．ｃｏｍ」に対応するアドレスを取得するために、ＤＮＳ　ｑｕｅｒｙ　ｆｏｒ“ｓｗａｎ．ｍｂｂ．ｎｉｆ．ｃｏｍ”をＤＮＳサーバに対して送信する。その結果、ＤＮＳサーバからは、ＤＮＳ　ａｎｓｗｅｒ：１５．２３．１．２が返送されてくるので、ルータＡは、ルータＢのアドレスを知ることになる。

【００５９】アドレスを受け取ったプライベート網宛名前解決判定部１３は、アドレス「１５．２３．１．２」を有するノードであるルータＢに対して受信端末である端末ＣのＩＰアドレスを問い合わせるために、ＤＮＳ　ｑｕｅｒｙ　ｆｏｒ“ＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍ”を送信する。

【００６０】ところで、ルータＢには、その配下に存在する端末Ｃ，Ｄに対してユニークな名前を付与して管理しているので、このような問い合わせがあった場合には、その名前に対応するＩＰアドレスを検索して返送する。いまの例では、端末Ｃに対するＩＰアドレス「１９２．１６８．０．２」が取得され、ＤＮＳ　ａｎｓｗｅｒ：１９２．１６８．０．２が返送されることになる。

【００６１】このようにして取得された端末ＣのＩＰアドレスは、プライベート網宛名前解決判定部１３に供給される。プライベート網宛名前解決判定部１３は、ダミーＩＰアドレスをダミーＩＰアドレスプール部１５から１つ取得するとともに、取得したＩＰアドレスが他の通信に重複して使用されることを防止するためにダミーＩＰアドレスプール部１５からそのダミーＩＰアドレスを削除する。例えば、いまの例では、ダミーアドレス「１０．０．０．１」が取得されるとともに、ダミーＩＰアドレスプール部１５から削除されることになる。

【００６２】続いて、プライベート網宛名前解決判定部１３は、取得したダミーＩＰアドレス「１０．０．０．１」を名前解決要求の回答として、端末Ａに対して送信する。ここで、端末Ｃのプライベートアドレスである「１９２．１６８．０．２」を回答として送付せずに、ダミーＩＰアドレスである「１０．０．０．１」を送信するのは、プライベートアドレスは異なるプライベート網間では重複する場合があるからである。そこで、本実施の形態では、そのような重複の発生を避けるために、ルータＡ配下のプライベートアドレス、即ち、クラスＣのプライベートアドレスとは異なるクラスＡのプライベートアドレスをダミーＩＰアドレスとして使用することとしている。

【００６３】インターネットでは通常使用されていないクラスＡのＩＰアドレスをダミーＩＰアドレスとして使用することとしている。続いて、プライベート網宛名前解決判定部１３は、受信許可ＩＰアドレス保持部１０ａに対してＩＰアドレス「１０．０．０．１」を受信してよいアドレスとして登録する。その結果、ＩＰアドレス「１０．０．０．１」を送信先アドレスとして含むパケットは受信の対象として許可されることになる。

【００６４】次に、プライベート網宛名前解決判定部１３は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に対して、受信端末である端末Ｃ、ルータＡ、ルータＢ、送信端末である端末ＡのＩＰアドレスをエントリとして登録する。具体的には、図３に示すように、「１９２．１６８．０．２／／３４．５６．１０．４：？？；１５．２３．１．２：？？／／１９２．１６８．０．１：？？；１０．０．０．１：？？／／×」がエントリとして登録されることになる。なお、ＩＰアドレスに続く「？？」の部分には、後述する処理により決定されるポート番号が登録され、また、最後の「×」は、通信許可フラグであり、通信が許可されない場合には「×」が、また、通信が許可される場合には「○」が登録される。

【００６５】次に、図５を参照して、ＴＣＰコネクションを確立する場合の処理について説明する。先ず、端末Ａが、ルータＡに対して、端末Ｃの２３番ポートとの間でＴＣＰのコネクションを確立するために、ＴＣＰのＳＹＮメッセージを１０．０．０．１のポート２３番に送信する。ここで、ソースアドレスは、図５に示すように、１９２．１６８．０．１：ＹＹ（ＳＲＣ＝１９２．１６８．０．１：ＹＹ）である。

【００６６】ルータＡのＩＰ部１０は、受信許可ＩＰアドレス保持部１０ａに１０．０．０．１が登録されているので、このパケットを受信し、ＴＣＰ部１１を介して、パケット転送部１７に供給する。

【００６７】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、１０．０．０．１に対応するエントリを取得する。その結果、１０．０．０．１が１５．２３．１．２の経由先であり、かつ、すべてのポート情報が定まっておらず、か

つ、通信許可フラグがオフの状態であるので、このコネクションは名前解決処理が終了しただけの状態であることを検出する。

【００６８】パケット転送部１７は、パケット転送用ＴＣＰコネクション管理部１８に対して、１５．２３．１．２を経由して１９２．１６８．０．２との間でＴＣＰコネクションを確立するように指示する。

【００６９】パケット転送部１７は、ＳＹＮメッセージに含まれているソースポートアドレス（ＹＹ）と、送信先ポート（２３）を通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の該当するエントリに対して追加する。

【００７０】パケット転送用ＴＣＰコネクション管理部１８は、１５．２３．１．２のポートＸＸとの間でＴＣＰコネクションをＴＣＰ部１１を介して確立する。即ち、パケット転送用ＴＣＰコネクション管理部１８は、ルータＢに対してＴＣＰのＳＹＮメッセージを１０．０．０．１のポート２３番（ＳＲＣ＝１９２．１６８．０．１：ＹＹ）に送信する。その結果、ルータＢから「ＳＹＮ＋ＡＣＫ」が返送されてくるので、パケット転送用ＴＣＰコネクション管理部１８は、「ＡＣＫ」をルータＢに対して送信する。なお、ここではＸＸはあらかじめ本手法用に割り当てられた任意の固定ポート値とする。その結果、ルータＢとルータＡとの間でＴＣＰコネクションが確立されることになる。

【００７１】次に、パケット転送用ＴＣＰコネクション管理部１８は、以上の処理によりルータＢとの間に確立されたコネクションを通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に登録する。即ち、パケット転送用ＴＣＰコネクション管理部１８は、ＴＣＰの送信元ポートと送信先ポートであるＷＷとＸＸを、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に登録する。その結果、先に示したエントリの「？？」が該当するポートに変更されることになる。

【００７２】次に、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末アドレス／ポートネゴシエーション部１９に対して、「１９２．１６８．０．２のポート２３番」を示すＮｏｔｉｆｉｃａｔｉｏｎメッセージ（ＭＳＧ）を、１５．２３．１．２のポートＸＸに対して、ポートＷＷのＴＣＰコネクションから送信するように指示する。

【００７３】通信先端末アドレス／ポートネゴシエーション部１９は、１９２．１６８．０．２のポート２３番を示すＮｏｔｉｆｉｃａｔｉｏｎメッセージを作成し、ルータＢに対して送信する。その結果、図５に示すように、ＮｏｔｉｆｉｃａｔｉｏｎメッセージがルータＢに対して送信されることになる。

【００７４】ルータＢのＴＣＰ部１１は、ポートＸＸを介して受信したＮｏｔｉｆｉｃａｔｉｏｎメッセージをパケット転送部１７に対して供給する。パケット転送部１７は、送信ポートＷＷから送信されてきたＳＹＮ，ＡＣＫ以外の最初のパケットであるため、これをＮｏｔｉｆｉｃａｔｉｏｎメッセージとみなして、パケット転送用ＴＣＰコネクション管理部１８に転送する。

【００７５】パケット転送用ＴＣＰコネクション管理部１８は、Ｎｏｔｉｆｉｃａｔｉｏｎメッセージに示されたアドレスとポート番号（アドレス１９２．１６８．１０．２の２３番ポート）との間で、ＴＣＰコネクションを確立する。即ち、パケット転送用ＴＣＰコネクション管理部１８は、端末Ｃに対してＴＣＰのＳＹＮメッセージを１９２．１６８．１０．２のポート２３番（ＳＲＣ＝１９２．１６８．０．１：ＹＹ）へ送信する。その結果、端末Ｃから「ＳＹＮ＋ＡＣＫ」が返送されてくるので、パケット転送用ＴＣＰコネクション管理部１８は、「ＡＣＫ」を端末Ｃに対して送信する。すると、端末ＣとルータＢとの間でコネクションが確立されることになる。

【００７６】ルータＢと端末Ｃとの間でコネクションが確立すると、ルータＢは、Ｎｏｔｉｆｉｃａｔｉｏｎメッセージに対する応答として、ＡＣＫメッセージをルータＡに対して返送するように要求する。

【００７７】その結果、ルータＢの通信先端末アドレス／ポートネゴシエーション部１９は、端末Ｃ（１９２．１６８．０．２）のポート２３番への接続完了を通知するＡＣＫメッセージをルータＡに対して送信する。

【００７８】続いて、ルータＢの通信先端末アドレス／ポートネゴシエーション部１９は、新たに確立されたコネクションに関するアドレス情報およびポート情報を通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に対して格納する。即ち、通信先端末アドレス／ポートネゴシエーション部１９は、新たに確立したコネクションの送信先アドレスとポート（１９２．１６８．０．２：２３）、ソースアドレスとポート（１０．０．０．１：ＺＺ）、Ｎｏｔｉｆｉｃａｔｉｏｎメッセージが送られてきたＴＣＰコネクションのソースアドレスとポート（３４．５６．１０．４：ＷＷ）、送信先アドレスとポート（１５．２３．１．２：ＸＸ）、および、オンの通信許可フラグを有するエントリを通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に書き込む。

【００７９】次に、ルータＡの通信先端末アドレス／ポートネゴシエーション部１９は、パケット転送用ＴＣＰコネクション管理部１８に対して、アドレス１９２．１６８．０．２のポート２３番へのコネクションが、１５．２３．１．２のポートＸＸから３４．５６．１０．４のポートＷＷへのＴＣＰコネクション経由で確立されたことを通知する。

【００８０】パケット転送用ＴＣＰコネクション管理部１８は、“３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ”をキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、該当する

エントリを取得する。そして取得したエントリに含まれている情報を参照することにより（図6参照）、通知されたＡＣＫメッセージに対する端末Ａとのコネクションが、１９２．１６８．０．１：ＹＹおよび１０．０．０．１：２３であることを検出する。

【００８１】パケット転送用ＴＣＰコネクション管理部１８は、ＴＣＰ部１１を介して、１９２．１６８．０．１：ＹＹと１０．０．０．１：２３との間で、コネクションを確立する。即ち、パケット転送用ＴＣＰコネクション管理部１８は、先ず、端末Ａに対してＳＹＮ＋ＡＣＫを送信し、その結果として端末Ａから返送されてきたＡＣＫを受信する。その結果、端末ＡとルータＡとの間でコネクションが確立されることになる（図6参照）。

【００８２】そして、最後に、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に登録されているエントリ「１９２．１６８．０．２／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／１９２．１６８．０．１：ＹＹ；１０．０．０．１：２３」の通信許可フラグをオフ（×）からオン（○）に変更する（図6参照）。

【００８３】ここで、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に登録されているエントリは、図7に示すように、受信端末、変更後送信先ＩＰアドレス、変更後送信先ポート、変更後送信先ＩＰアドレス、変更後送信先ポート、変更前送信先ＩＰアドレス、変更前送信先ポート、変更前送信元ＩＰアドレス、変更前送信元ポート、および、通信許可フラグによって構成されている。

【００８４】「受信端末」は、この例では、端末ＣのＩＰアドレス（１９２．１６８．０．２）であり、インターネット上においてＴＣＰコネクションを確立する側のルータのみが保持している情報である。

【００８５】「変更後送信元ＩＰアドレス」および「変更後送信元ポート」は、アドレス変換後の送信元ＩＰアドレスおよび送信元ポート番号である。この例では、ルータＡのＩＰアドレスである３４．５６．１０．４と、ポート番号ＷＷとが該当する。

【００８６】「変更後送信先ＩＰアドレス」および「変更後送信先ポート」は、アドレス変換後の送信先ＩＰアドレスおよび送信先ポート番号である。この例では、ルータＢのＩＰアドレスである１５．２３．１．２と、ポート番号ＸＸとが該当する。

【００８７】「変更前送信元ＩＰアドレス」および「変更前送信元ポート」は、アドレス変換前の送信元ＩＰアドレスおよび送信元ポート番号である。この例では、端末Ａのアドレスである１９２．１６８．０．１と、ポート番号ＹＹとが該当する。

【００８８】「変更前送信先ＩＰアドレス」および「変更前送信先ポート」は、アドレス変換前の送信先ＩＰアドレスおよび送信先ポート番号である。この例では、ダミーＩＰアドレスである１０．０．０．１と、ポート２３番とが該当する。

【００８９】「通信許可フラグ」は、当該エントリが通信を許可されているか否かを示す情報であり、通信許可の場合には“○”、不許可の場合には“×”、一方向の通信がなされている場合には“△”となる。

【００９０】次に、図8を参照して、以上の処理によって確立されたＴＣＰコネクションを利用してパケットを転送する場合の処理について説明する。先ず、端末Ａから、送信先が１０．０．０．１：２３であり、また、送信元が１９２．１６８．０．１：ＹＹであることを示すヘッダが付与されたパケット（ＴＣＰ　ｄａｔａ　ｔｏ　１０．０．０．１：２３（ＳＲＣ＝１９２．１６８．０．１：ＹＹ））がルータＡに対して送信されると、ルータＡは、これを受信する。

【００９１】ルータＡのＩＰ部１０は、１０．０．０．１：２３が受信許可ＩＰアドレス保持部１０ａに保持されていることから、これを受信し、ＴＣＰ部１１を介してパケット転送部１７に転送する。

【００９２】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索して該当するエントリを取得する。いまの例では、図8に示すエントリ「１９２．１６８．０．２／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／１９２．１６８．０．１：ＹＹ；１０．０．０．１：２３／／○」が取得される。そして、このエントリに格納されている情報を参照し、パケットのヘッダに含まれている送信先ＩＰアドレスおよびポート情報である１０．０．０．１：２３を、１５．２３．１．２：ＸＸに変換し、また、送信元ＩＰアドレスおよびポート情報である１９２．１６８．０．１：ＹＹを３４．５６．１０．４：ＷＷに変換する。なお、パケットのデータグラムについては特に変更しない。

【００９３】パケット転送部１７は、ヘッダの変換が終了したパケットを、ＴＣＰ部１１を介してルータＢに向けて送信する。ルータＢは、ルータＡから伝送されてきたパケットを受信し、ポートＸＸを介して読み込み、パケット転送部１７に供給する。

【００９４】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、受信したパケットに対応するエントリである「ＮＵＬＬ／／１０．０．０．１：ＺＺ；１９２．１６８．０．２：２３／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／○」を取得する。そして、パケット転送部１７は、取得したエントリに含まれている情報を参照し、パケットのヘッダに付加されている送信先ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを１９２．１６８．０．２：２３に変換し、送信元ＩＰアドレスおよびポート情報である１９２．１６８．

０．１：ＹＹを１０．０．０．１：ＺＺに変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介して端末Ｃに対して送信する。

【００９５】その結果、端末Ａから送信されたパケットは、プライベートアドレス網に属する端末Ｃに到達することになる。次に、端末Ｃは、受信したパケットに対する応答としてのパケットを生成し、その送信先ＩＰアドレスおよびポートを１０．０．０．１：ＺＺに、また、送信元ＩＰアドレスおよびポートを１９２．１６８．１０．２：２３に設定し、送信する。なお、送信先ＩＰアドレスとして１０．０．０．１：２３を使用するのは、端末Ｃが属しているプライベートアドレス網の他のノードに誤って配信されることを防止するためである。

【００９６】端末Ｃから送信されたパケットは、ルータＢによって受信され、ＩＰ部１０に対して供給される。ＩＰ部１０は、１０．０．０．１：ＺＺが受信許可ＩＰアドレス保持部１０ａに保持されていることから、このパケットを受信し、ＴＣＰ部１１を介してパケット転送部１７に転送する。

【００９７】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索して該当するエントリを取得する。いまの例では、図８に示す「ＮＵＬＬ／／１０．０．０．１：ＺＺ；１９２．１６８．０．２：２３／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／○」が取得される。そして、このエントリに格納されている情報を参照し、パケットのヘッダに含まれている送信先ＩＰアドレスおよびポート情報である１０．０．０．１：ＺＺを、３４．５６．１０．４：ＷＷに変換し、また、送信元ＩＰアドレスおよびポート情報である１９２．１６８．１０．２：２３を、１５．２３．１．２：ＸＸに変換する。なお、パケットのデータグラムについては特に変更しない。

【００９８】パケット転送部１７は、ヘッダの変換が終了したパケットを、ＴＣＰ部１１を介してルータＡに向けて送信する。ルータＡは、ルータＢから伝送されてきたパケットを受信し、ポートＷＷを介して読み込み、パケット転送部１７に供給する。

【００９９】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、受信したパケットに対応するエントリである「１９２．１６８．０．２／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／１９２．１６８．０．１：ＹＹ；１０．０．０．１：２３／／○」を取得する。そして、パケット転送部１７は、取得したエントリに含まれている情報を参照し、パケットのヘッダに付加されている送信先ＩＰアドレスおよびポート情報である３４．５６．１０．４：ＷＷを、１９２．１６８．０．１：ＹＹに変換し、また、送信元ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを、１０．０．０．１：２３に変換し、パケットのデータグラムは変更せずに、ＴＣＰ部１１を介して端末Ａに対して送信する。

【０１００】その結果、端末Ｃから送信されたパケットは、プライベートアドレス網に属する端末Ａに到達することになる。以上のような処理により、それぞれプライベートアドレス網に属する端末Ａと端末Ｃとの間でパケットの授受を行なうことが可能になる。

【０１０１】次に、図９および図１０を参照して、ＴＣＰコネクションを終了する場合の処理について説明する。先ず、図９を参照して、双方向の通信を片方向に変更する場合の処理について説明する。

【０１０２】端末ＡからＴＣＰコネクションを終了するためにＴＣＰのＦＩＮメッセージが１０．０．０．１のポート２３番（ＳＲＣ＝１９２．１６８．０．１：ＹＹ）へ送信されると、ルータＡは、２３番ポートを介してこのメッセージを受信する。

【０１０３】ルータＡのＩＰ部１０は、受信したパケットのヘッダに付加されている送信先アドレスである１０．０．０．１が受信許可ＩＰアドレス保持部１０ａに格納されているので、受信許可パケットと判断して、ＴＣＰ部１１を介してパケット転送部１７に供給する。

【０１０４】パケット転送部１７は、パケット転送用ＴＣＰコネクション管理部１８に、送信先ＩＰアドレスおよびポート情報が１０．０．０．１：２３であり、送信元ＩＰアドレスおよびポート情報が１９２．１６８．０．１：ＹＹであるＴＣＰコネクションからＦＩＮメッセージがきたことを通知する。

【０１０５】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１０．０．０．１：２３を１５．２３．１．２：ＸＸに変換し、また、送信元ＩＰアドレスおよびポート情報である１９２．１６８．０．１：ＹＹを３４．５６．１０．４：ＷＷに変換し、パケットのデータグラムは変更せずに、ＴＣＰ部１１を経由して、ルータＢに送信する。

【０１０６】パケットの送信が完了すると、ルータＡのパケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポートが３４．５６．１０．４：ＷＷであり、送信元ＩＰアドレスおよびポートが１５．２３．１．２：ＸＸであるコネクションからのＦＩＮメッセージに対する応答メッセージであるＡＣＫメッセージが到着するのを待つ。

【０１０７】ルータＢは、ルータＡから送信されたパケットをポートＸＸを介して受信し、パケット転送部１７に供給する。パケット転送部１７は、送信先ＩＰアドレスおよびポートが１５．２３．１．２：ＸＸであり、送信元ＩＰアドレスおよびポートが３４．５６．１０．４：ＷＷであるＴＣＰコネクションからＦＩＮメッセージが到着したことをパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１０８】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを１９２．１６８．０．２：２３に変換し、送信元ＩＰアドレスおよびポート情報である３４．５６．１０．４．WWを１０．０．０．１：ＺＺに変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介してパケットを端末Ｃに送信する。

【０１０９】そして、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレス・ポートが１０．０．０．１：ＺＺであり、送信元ＩＰアドレス・ポートが１９２．１６８．０．２：２３であるコネクションからのＦＩＮに対するＡＣＫメッセージが返送されるのを待つ。

【０１１０】続いて、端末Ｃは、ルータＢから送信されたＦＩＮメッセージを受信し、その応答であるＴＣＰのＡＣＫメッセージを１０．０．０．１のポートＺＺ番（ＳＲＣ＝１９２．１６８．１０．２：２３）へ送信する。

【０１１１】ルータＢは、端末Ｃから送信されたパケットをポートＺＺを介して受信し、パケット転送部１７に供給する。パケット転送部１７は、送信先ＩＰアドレスおよびポートが１０．０．０．１：ＺＺであり、送信元ＩＰアドレスおよびポートが１９２．１６８．１０．２：２３あるＴＣＰコネクションからＡＣＫメッセージが到着したことをパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１１２】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１０．０．０．１：ＺＺを３４．５６．１０．４：WWに変換し、送信元ＩＰアドレスおよびポート情報である１９２．１６８．１０．２：２３を、１５．２３．１．２：WWに変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介してルータＡに送信する。

【０１１３】そして、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に格納されている該当するエントリ「ＮＵＬＬ／／１０．０．０．１：ＺＺ；１９２．１６８．０．２：２３／／３４．５６．１０．４：WW；１５．２３．１．２：ＸＸ／／○」に通信許可フラグを「通信許可」の状態から「一方向」を示す「△」に変更する。

【０１１４】その結果、端末ＣとルータＢとの間のコネクションがＯｎｅ－ｗａｙ　Ｃｏｎｎｅｃｔｉｏｎの状態になる。ルータＡは、ルータＢから送信されたパケットをポートWWを介して受信し、パケット転送部１７に供給する。

【０１１５】パケット転送部１７は、送信先ＩＰアドレスおよびポートが３４．５６．１０．４：WWであり、送信元ＩＰアドレスおよびポートが１５．２３．１．２：ＸＸであるＴＣＰコネクションからＡＣＫメッセージが到着したことをパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１１６】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である３４．５６．１０．４：WWを１９２．１６８．０．１：ＹＹに変換し、送信元ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを、１０．０．０．１：２３に変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介して端末Ａに送信する。

【０１１７】そして、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に格納されている該当するエントリ「１９２．１６８．０．２／／３４．５６．１０．４：WW；１５．２３．１．２：ＸＸ／／１９２．１６８．０．１：ＹＹ；１０．０．０．１：２３／／○」の通信許可フラグを「通信許可」を示す「○」から「一方向」を示す「△」に変更する。

【０１１８】その結果、ルータＢとルータＡおよびルータＡと端末Ａとの間のコネクションがＯｎｅ－ｗａｙ　Ｃｏｎｎｅｃｔｉｏｎの状態になる。次に、図１０を参照して、ＴＣＰコネクションを片方向から終了させる場合の処理について説明する。

【０１１９】端末ＣからＴＣＰコネクションを終了するためにＴＣＰのＦＩＮメッセージが１０．０．０．１のポートＺＺ番（ＳＲＣ＝１９２．１６８．０．２：２３）へ送信されると、ルータＢは、ＺＺ番ポートを介してこのメッセージを受信する。

【０１２０】ルータＢのＩＰ部１０は、受信したパケットのヘッダに付加されている送信先アドレスである１０．０．０．１が受信許可ＩＰアドレス保持部１０ａに格納されているので、受信可能のパケットと判断して、ＴＣＰ部１１を介してパケット転送部１７に供給する。

【０１２１】パケット転送部１７は、パケット転送用ＴＣＰコネクション管理部１８に、送信先ＩＰアドレスおよびポート情報が１０．０．０．１：ＺＺであり、送信元ＩＰアドレスおよびポート情報が１９２．１６８．０．２：２３であるＴＣＰコネクションからＦＩＮメッセージが到着したことを通知する。

【０１２２】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１０．０．０．１：ＺＺを３４．５６．１０．４：WWに変換し、また、送信元ＩＰアドレスおよびポート情報である１９２．１６８．０．２：２３を１５．２３．１．２：ＸＸに変換し、パケットのデータグラムは変更せずに、ＴＣＰ部１１を経由して、ルータＡに送信する。

【０１２３】パケットの送信が完了すると、ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポートが１５．２３．１．２：ＸＸであり、送信元ＩＰアドレスおよびポートが３４．５６．１０．４：ＷＷであるコネクションからのＦＩＮメッセージに対する応答メッセージであるＡＣＫメッセージが到着するのを待つ。

【０１２４】ルータＡは、ルータＢから送信されたパケットをポートＷＷを介して受信し、パケット転送部１７に供給する。ルータＡのパケット転送部１７は、送信先ＩＰアドレスおよびポートが３４．５６．１０．４：ＷＷであり、送信元ＩＰアドレスおよびポートが１５．２３．１．２：ＸＸであるＴＣＰコネクションからＦＩＮメッセージが到着したことをパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１２５】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である３４．５６．１０．４：ＷＷを１９２．１６８．０．１：ＹＹに変換し、送信元ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを１０．０．０．１：２３に変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介してパケットを端末Ａに送信する。

【０１２６】そして、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポートが１０．０．０．１：２３であり、送信元ＩＰアドレス・ポートが１９２．１６８．０．１：ＹＹであるコネクションからのＦＩＮに対するＡＣＫメッセージが返送されるのを待つ。

【０１２７】端末ＡからＦＩＮメッセージに対する応答としてＴＣＰのＡＣＫメッセージが１０．０．０．１のポート２３番（ＳＲＣ＝１９２．１６８．０．１：ＹＹ）」へ送信されると、ルータＡはこれを受信し、パケット転送部１７に供給する。

【０１２８】パケット転送部１７は、送信先ＩＰアドレスおよびポート情報が１０．０．０．１：２３であり、送信元ＩＰアドレスおよびポート情報が１９２．１６８．１０．１：ＹＹあるＴＣＰコネクションからＡＣＫメッセージが到着したことをパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１２９】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１０．０．０．１：２３を１５．２３．１．２：ＸＸに変換し、送信元ＩＰアドレスおよびポート情報である１９２．１６８．１０．１：ＹＹを、３４．５６．１０．４：ＷＷに変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介してルータＢに送信する。

【０１３０】そして、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に格納されている該当するエントリ「１９２．１６８．０．２／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／１９２．１６８．０．１：ＹＹ；１０．０．０．１：２３／／△」を削除する。

【０１３１】その結果、端末ＡとルータＡとの間のコネクションがＯｎｅ－ｗａｙ　Ｃｏｎｎｅｃｔｉｏｎの状態からＣｏｎｎｅｃｔｉｏｎ　Ｃｌｏｓｅの状態になる。更に、ルータＡのパケット転送用ＴＣＰコネクション管理部１８は、受信許可ＩＰアドレス保持部１０ａに、エントリの変更前送信先ＩＰアドレスに記載されているダミーアドレス、即ち、１０．０．０．１の受信中止を通知し、ダミーＩＰアドレスプール部１５にダミーアドレスを返却する。

【０１３２】ルータＢは、ルータＡから送信されたパケットをポートＸＸを介して受信し、パケット転送部１７に供給する。パケット転送部１７は、送信先ＩＰアドレスおよびポート情報が１５．２３．１．２：ＸＸであり、送信元ＩＰアドレスおよびポート情報が３４．５６．１０．４：ＷＷであるＴＣＰコネクションからＡＣＫメッセージが到着したことをパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１３３】パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを１９２．１６８．０．２：２３に変換し、送信元ＩＰアドレスおよびポート情報である３４．５６．１０．４：ＷＷを、１０．０．０．１：ＺＺに変換し、パケットのデータグラムは変換せずに、ＴＣＰ部１１を介して端末Ｃに送信する。

【０１３４】そして、パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に格納されている該当するエントリ「１９２．１６８．０．２／／３４．５６．１０．４：ＷＷ；１５．２３．１．２：ＸＸ／／１９２．１６８．０．１：ＹＹ；１０．０．０．１：２３／／△」を削除する。

【０１３５】その結果、端末ＣとルータＢおよびルータＢとルータＡとの間のコネクションがＯｎｅ－ｗａｙ　Ｃｏｎｎｅｃｔｉｏｎの状態からＣｏｎｎｅｃｔｉｏｎ　Ｃｌｏｓｅの状態になる。更に、ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、受信許可ＩＰアドレス保持部１０ａに、エントリの変更後送信元ＩＰアドレスに記載されているダミーアドレス、即ち、１０．０．０．１の受信中止を通知し、ダミーＩＰアドレスプール部１５にダミーアドレスを返却する。

【０１３６】以上の処理により、一旦確立されたコネクションを終了することが可能になる。次に、図１１およ

び図１２を参照して、ＴＣＰコネクションが何らかの原因で切断された場合における復旧処理について説明する。

【０１３７】図１１は、ルータＡとルータＢの間のコネクションが切断した場合における復旧処理について説明する図である。この図に示すように、ルータＡとルータＢの間のコネクションが切断すると、ルータＡのＴＣＰ部１１およびルータＢのＴＣＰ部１１は、コネクションが切断したことを検出する。

【０１３８】コネクションの切断を検出したルータＡのＴＣＰ部１１は、切断されたコネクションの両端(ルータＡとルータＢ)のそれぞれのＩＰアドレスとポート番号をパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１３９】ルータＡのパケット転送用ＴＣＰコネクション管理部１８はＴＣＰ部１１から受け取ったデータをキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、検索結果のエントリの“通信許可フラグ”をオフにする。また、“受信端末”フィールドがＮＵＬＬではないことから、自己がＴＣＰを主体的に確立したノードであることを了知し、ルータＢのポートＸＸとの間で、ＴＣＰコネクションを確立するようにＴＣＰ部１１に指示する。

【０１４０】その結果、ＴＣＰ部１１は、ルータＢに対してコネクションを確立するためにＴＣＰのＳＹＮメッセージを１５．２３．１．２のポートＸＸ番（ＳＲＣ＝３４．５６．１０．４：ＶＶ）へ送信する。

【０１４１】このとき、ルータＢでは、パケット転送用ＴＣＰコネクション管理部１８がＴＣＰ部１１から受け取ったデータをキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、検索結果のエントリの“通信許可フラグ”をオフにする。また、“受信端末”フィールドがＮＵＬＬであることから、自己がＴＣＰを主体的に確立したノードでないことを了知し、ルータＡからのコネクションの再設定を待つ。

【０１４２】そして、ルータＢにルータＡから送信されたＳＹＮメッセージが届くと、ルータＢは、ＳＹＮ＋ＡＣＫメッセージをルータＡに対して送信する。その結果、ルータＡからは、ＡＣＫメッセージが返送され、これらの間のコネクションが再度確立（Ｒｅ－ｅｓｔａｂｌｉｓｈｍｅｎｔ）されることになる。

【０１４３】ルータＡとルータＢの間のコネクションが再確立されると、ルータＡはルータＢに対して前述の場合と同様に、Ｎｏｔｉｆｉｃａｔｉｏｎメッセージを送信する。

【０１４４】Ｎｏｔｉｆｉｃａｔｉｏｎメッセージを受信したルータＢは、Ｎｏｔｉｆｉｃａｔｉｏｎメッセージに対するＡＣＫを送信し、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の対応するエントリの変更前送信元ポートを新しいポート番号（ＶＶ）に書換え、通信許可フラグをオンにする。

【０１４５】一方、ルータＡは、ＡＣＫメッセージを受信し、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の対応するエントリの送信変更後送信元ポートを新しいポート番号（ＶＶ）に書換え、通信許可フラグをオンにする。

【０１４６】以上の処理により、ルータＡとルータＢの間のコネクションが切断された場合でも、コネクションを再確立し、通信を継続することが可能になる。次に、図１２を参照して、ルータＢと端末Ｃの間のコネクションが切断した場合における復旧処理について説明する。

【０１４７】ルータＢと端末Ｃとの間のコネクションが何らかの原因で切断すると、ルータＢのＴＣＰ部１１がこれを検出する。ルータＢのＴＣＰ部１１は、切断されたコネクションの両端（ルータＢと端末Ｃ）のそれぞれのＩＰアドレスとポート番号をパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０１４８】パケット転送用ＴＣＰコネクション管理部１８は、ＴＣＰ部１１から通知されたデータをキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、検査結果のエントリの“通信許可フラグ”をオフにする。また、端末Ｃのポート２３番との間で、ＴＣＰコネクションを確立するように、ＴＣＰ部１１に指示する。

【０１４９】その結果、ルータＢから端末Ｃに対して、ＴＣＰのＳＹＮメッセージが１９２．１６８．０．２のポート２３番（ＳＲＣ＝１０．０．０．１：ＵＵ）へ送信される。

【０１５０】すると、端末Ｃは、このＳＹＮメッセージを受信し、応答メッセージであるＳＹＮ＋ＡＣＫメッセージをルータＢに対して返信する。端末ＣからのＳＹＮ＋ＡＣＫメッセージを受信したルータＢは、ＡＣＫメッセージを端末Ｃに対して送信するとともに、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の該当するエントリの変更後送信元ポートを新たなポート番号（ＵＵ）に変更し、また、通信許可フラグをオンの状態にする。

【０１５１】以上の処理により、ルータＢと端末Ｃとの間のコネクションが何らかの原因によって切断した場合であっても、これを復旧して通信を継続することが可能になる。なお、ルータＡと端末Ａ間でＴＣＰコネクションが何らかの原因で切断された場合も同様に復旧処理を行う。

【０１５２】最後に、以上に説明した実施の形態において実行される処理の流れについてフローチャートを参照して説明する。図１３は、図２に示す名前解決処理が実行される際のルータＡにおける処理の流れを説明するフローチャートである。このフローチャートは、ルータＡに名前解決要求が到着した場合に実行される処理であり、以下では、ルータＡに名前解決要求「ＰＣ－Ｂ．ｈ

ｏｍｅ．ｃｏｍ」が到着した場合を例に挙げて説明する。

【０１５３】ステップＳ１０：名前解決部１２は、端末Ａから送信された名前解決要求である「ＰＣ－Ｂ．ｈｏｍｅ．ｃｏｍ」を通信手段２０、ＩＰ部１０、および、ＴＣＰ部１１を介して受信する。

【０１５４】ステップＳ１１：名前解決部１２は、この要求をプライベート網宛名前解決判定部１３へ転送する。

【０１５５】ステップＳ１２：プライベート網宛名前解決判定部１３は、通信先プライベート網用名前解決サーバ登録部１４を検索し、問合せ先アドレスのエントリが登録されているか否かを判定し、登録されていると判定した場合にはステップＳ１４に進み、それ以外の場合にはステップＳ１３に進む。

【０１５６】ステップＳ１３：名前解決部１２は、通常の名前解決要求として受け付けた要求を処理する。

ステップＳ１４：プライベート網宛名前解決判定部１３は、ルータＢ（ｓｗａｎ．ｍｂｂ．ｎｉｆｔｙ．ｃｏｍ）のＩＰアドレスをグローバル網上の所定のＤＮＳサーバに問い合わせるよう名前解決部へ指示する。

【０１５７】ステップＳ１５：プライベート網宛名前解決判定部１３は、ＤＮＳサーバから返送されてきた問い合せ結果（１５．２３．１．２）を通信手段２０、ＩＰ部１０、ＴＣＰ部１１、および、名前解決部１２を介して受信する。

【０１５８】ステップＳ１６：プライベート網宛名前解決判定部１３は、受信端末Ｂ（ＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍ）のＩＰアドレスを１５．２３．１．２（ルータＢ）に問い合わせるよう名前解決部１２に指示する。

【０１５９】ステップＳ１７：プライベート網宛名前解決判定部１３は、ルータＢから返送されてきた問合せ結果（１９２．１６８．０．２）を通信手段２０、ＩＰ部１０、ＴＣＰ部１１、および、名前解決部１２を介して受信する。

【０１６０】ステップＳ１８：プライベート網宛名前解決判定部１３は、ダミーＩＰアドレスプール部１５から任意のダミーＩＰアドレス（例えば、１０．０．０．１）を選択し、そのアドレスをダミーＩＰアドレスプール部から削除する。

【０１６１】ステップＳ１９：プライベート網宛名前解決判定部１３は、端末Ａにダミーのアドレス（１０．０．０．１）を名前解決要求の回答として送信する。

【０１６２】ステップＳ２０：プライベート網宛名前解決判定部１３は、ダミーＩＰアドレスを送信先アドレスとして有するパケットをプライベート網側から受信するように受信許可ＩＰアドレス保持部１０ａに指示する。

【０１６３】ステップＳ２１：プライベート網宛名前解決判定部１３は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に、端末Ｂ、ルータＡ、ルータＢ、および、端末Ａのそれぞれのアドレスと、ダミーＩＰアドレスをエントリとして登録する。但し、通信許可フラグについては、オフの状態に設定する。

【０１６４】次に、図１４を参照して、ＴＣＰコネクションを確立する際の処理について説明する。なお、以下の説明では、ルータＡとルータＢの間でＴＣＰコネクションを確立する場合の処理を例に挙げて説明する。ルータＡに端末Ａから送信先ＩＰアドレスが１０．０．０．１であり、送信先ポートが２３番であるＴＣＰのＳＹＮが到着すると、以下のステップが開始される。

【０１６５】ステップＳ３０：ルータＡのＩＰ部１０は、受信許可ＩＰアドレス保持部１０ａを参照し、ＩＰアドレス「１０．０．０．１」が登録されていることからこのパケットを受信し、ＴＣＰ部１１を介してパケット転送部１７に供給する。

【０１６６】ステップＳ３１：パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６から経由先を検索する。即ち、パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、ＩＰアドレス１０．０．０．１が、ＩＰアドレス１５．２３．１．２の経由先にあることを検出する。また、このとき、全てのポート情報のエントリが埋まっておらず、かつ、通信許可フラグがオフであるので、名前解決が終わっただけの状態であることを検出する。

【０１６７】ステップＳ３２：パケット転送部１７は、パケット転送用ＴＣＰコネクション管理部１８に対して、ＩＰアドレス１５．２３．１．２とＩＰアドレス１９２．１６８．０．２の間にＴＣＰコネクションを確立するように指示する。

【０１６８】ステップＳ３３：パケット転送用ＴＣＰコネクション管理部１８は、ＩＰアドレス１５．２３．１．２のポートＸＸとの間でＴＣＰコネクションを確立する。その結果、後述するステップＳ４０との間の処理により、ルータＢとルータＡとの間でコネクションが確立されることになる。

【０１６９】ステップＳ３４：パケット転送用ＴＣＰコネクション管理部１８は、ステップＳ３３において確立されたコネクションに関するＴＣＰの送信元と送信先ポート（ＷＷとＸＸ）を通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の該当するエントリに書き込む。

【０１７０】ステップＳ３５：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末アドレス／ポートネゴシエーション部１９に、１９２．１６８．０．２のポート２３番に関するＮｏｔｉｆｉｃａｔｉｏｎメッセージを１５．２３．１．２のポートＸＸに対して、ポートＷＷのＴＣＰコネクションから送信するように指示す

る。
【0171】ステップS36：通信先端末アドレス／ポートネゴシエーション部19は、192．168．0．2のポート23番に関するNotificationメッセージを15．23．1．2のポートXXにポートWWのTCPコネクションから送信する。
【0172】ステップS40：前述したステップS33の処理に基づいて、ルータBにおいても、TCPコネクションが確立される。
【0173】ステップS41：TCP部は、ポートXXで受信したNotificationメッセージをパケット転送部17へ供給する。そして、パケット転送部17は、送信ポートWWから送信されてきたSYN，ACK以外の最初のパケットであるため、これをNotificationメッセージとみなして、パケット転送用TCPコネクション管理部18へ供給する。
【0174】ステップS42：パケット転送用TCPコネクション管理部18は、Notificationメッセージで示されたアドレスとポート（192．168．10．2の23番）との間で、TCPコネクションを確立する。
【0175】ステップS43：パケット転送用TCPコネクション管理部18は、通信先端末アドレス／ポートネゴシエーション部19に34．56．10．4のポートWW番へACKメッセージを送信するように指示し、通信先端末アドレス／ポートネゴシエーション部19により、既に確立されているTCPコネクションを介して送信される。
【0176】ステップS44：通信先端末アドレス／ポートネゴシエーション部19は、確立されたTCPの送信先アドレスとポート（192．168．0．2：23）、ソースアドレスとポート（10．0．0．1：ZZ）、Notificationメッセージが送られてきたTCPコネクションのソースアドレスとポート（34．56．10．4：WW）、送信先アドレスとポート（15．23．1．2：XX）、および、オンの通信許可フラグを有するエントリを通信先端末・ゲートウェイIPアドレス／ポート保持部16に書き込み、図15の（1）に進む。
【0177】続いて、図15を参照して以上の処理の続きについて説明する。ステップS50：ルータAの通信先端末アドレス／ポートネゴシエーション部19は、パケット転送用TCPコネクション管理部18に、192．168．0．2のポート23番へのコネクションが、15．23．1．2のポートXXからポートWWのTCPコネクション経由で確立した旨を通知する。
【0178】ステップS51：パケット転送用TCPコネクション管理部18は、通信先端末・ゲートウェイIPアドレス／ポート保持部16を“34．56．10．4／WW；15．23．1．2：XX”をキーとして検索し、これの送信端末側とのTCPコネクションが192．168．0．1：YY、10．0．0．1：23であることを検知する。
【0179】ステップS52：パケット転送用TCPコネクション管理部18は、TCP部11を介して192．168．0．1：YYと10．0．0．1：23との間でのTCPコネクションを確立する。
【0180】ステップS53：パケット転送用TCPコネクション管理部18は、通信先端末・ゲートウェイIPアドレス／ポート保持部16に登録されているエントリ「192．168．0．2／／34．56．10．4：WW；15．23．1．2：XX／／192．168．0．1：YY；10．0．0．1：23」の通信許可フラグをオンに変更する。
【0181】以上の処理により、ルータAとルータBとの間にPCTコネクションを確立することが可能になる。次に、図16を参照し、以上のような処理によって確立されたTCPコネクションを利用してパケットを転送する際の処理について説明する。なお、以下では、ルータAとルータBの間におけるパケットの転送処理を例に挙げて説明する。
【0182】ステップS60：端末Aからルータに、送信先アドレスが10．0．0．1であり、また、送信先ポートが23番であるTCPのDATAパケットが到着する。
【0183】ステップS61：ルータAのIP部10は、10．0．0．1が受信許可IPアドレス保持部10aに登録されているためにこれを受信し、TCP部11を介してしてパケット転送部17へ渡す。
【0184】ステップS62：パケット転送部17は、通信先端末・ゲートウェイIPアドレス／ポート保持部16を検索し、送信先IPアドレス・ポート情報である10．0．0．1：23を15．23．1．2：XXに、送信元IPアドレス・ポート情報である192．168．0．1：YYを34．56．10．4：WWに変更し、パケットのデータグラムはそのままとする。
【0185】ステップS63：パケット転送部17は、アドレスの変換が終了したパケットをTCP部11を介して送信する。
【0186】ステップS70：ルータAからルータBのXX番ポートにTCPのDATAパケットが到着する。
【0187】ステップS71：ルータBのTCP部11は、ポートXXに到着したDATAパケットを受信し、パケット転送部17へ渡す。
【0188】ステップS72：パケット転送部17は、通信先端末・ゲートウェイIPアドレス／ポート保持部16を検索し、送信先IPアドレスおよびポート情報である15．23．1．2：XXを192．168．0．2：23に、送信元IPアドレス・ポート情報である192．168．0．1：YYを10．0．0．1：ZZ

に変換し、パケットのデータグラムはそのままとする。
【０１８９】ステップＳ７３：パケット転送部１７は、アドレスの変換が終了したパケットを、ＴＣＰ部１１を介してＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍ（端末Ｃ）に送信する。
【０１９０】以上の処理により、ＴＣＰコネクションを利用してパケットを転送することが可能になる。次に、図１７を参照して、ＴＣＰコネクションを終了する際にルータＡおよびルータＢにおいて実行される処理について説明する。
【０１９１】ステップＳ８０：ルータＡに端末Ａから送信先アドレスが１０．０．０．１であり、送信先ポートが２３番であるＴＣＰのＦＩＮパケットが到着する。
【０１９２】ステップＳ８１：ルータＡのＩＰ部１１は、１０．０．０．１が受信許可ＩＰアドレス保持部１０ａに登録されているのでこれを受信し、ＴＣＰ部１１を介してパケット転送部１７へ渡す。そして、ステップＳ８３とステップＳ８２の処理を並行して実行する。
【０１９３】ステップＳ８２：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレス・ポートが３４．５６．１０．４．ＷＷであり、送信元ＩＰアドレス・ポートが１５．２３．１．２：ＸＸであるコネクションからのＦＩＮに対するＡＣＫメッセージを受信したか否かを判定し、受信した場合には図１８の（２）に進み、それ以外の場合には同様の処理を繰り返す。
【０１９４】ステップＳ８３：パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレス・ポート情報である１０．０．０．１：２３を１５．２３．１．２：ＸＸに、送信元ＩＰアドレス・ポート情報である１９２．１６８．０．１：ＹＹを３４．５６．１０．４：ＷＷに変換し、パケットのデータグラムはそのままの状態とし、ＴＣＰ部１１を介してルータＢに転送する。
【０１９５】ステップＳ９０：ルータＢのＸＸ番ポートにルータＡからＴＣＰのＦＩＮパケットが到着する。
ステップＳ９１：ＴＣＰ部１１はポートＸＸで受信したＦＩＮパケットをパケット転送部１７へ渡す。そして、パケット転送部１７は、パケット転送用ＴＣＰコネクション管理部１８に、送信先ＩＰアドレスおよびポートが１５．２３．１．２：ＸＸであり、送信元ＩＰアドレスおよびポートが３４．５６．１０．４．ＷＷであるＴＣＰコネクションからＦＩＮが到着したことを通知した後、ステップＳ９２とステップＳ９３の処理を並行して実行する。
【０１９６】ステップＳ９２：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポートが１０．０．０．１．ＺＺであり、送信元ＩＰアドレスおよびポートが１９２．１６８．０．２．２３であるコネクションからのＦＩＮに対するＡＣＫメッセージが受信されたか否かを判定し、受信された場合には図１８の（３）に進み、それ以外の場合には同様の処理を繰り返す。
【０１９７】ステップＳ９３：パケット転送部１７は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、送信先ＩＰアドレスおよびポート情報である１５．２３．１．２：ＸＸを１９２．１６８．０．２：２３に、送信元ＩＰアドレスおよびポート情報である３４．５６．１０．４．ＷＷを１０．０．０．１：ＺＺに変換し、パケットのデータグラムは変更せずに、ＴＣＰ部１１を介してＰＣ－Ｂ．ｈｏｍｅ－ａ．ｃｏｍへ送信する。
【０１９８】続いて、図１８を参照して、以上の処理の続きについて説明する。ステップＳ１００：ルータＢと同様の動作、即ち、後述のステップＳ１１０～Ｓ１１７の処理により、ＡＣＫパケットの転送および通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６のエントリの変更または削除を行なう。
【０１９９】ステップＳ１１０：ルータＢに、ＡＣＫパケットが到着する。
ステップＳ１１１：ルータＢのＩＰ部１０は、ＡＣＫパケットに含まれているアドレス１０．０．０．１が、受信許可ＩＰアドレス保持部１０ａに登録されているのでこれを受信し、ＴＣＰ部１１を介してパケット転送部１７へ渡す。
【０２００】ステップＳ１１２：パケット転送部１７は、パケット転送用ＴＣＰコネクション管理部１８に、送信先ＩＰアドレスおよびポートが１０．０．０．１：ＺＺであり、送信元ＩＰアドレスおよびポートが１９２．１６８．０．２：２３であるＴＣＰコネクションからＡＣＫが到着したことを通知する。
【０２０１】ステップＳ１１３：パケット転送用ＴＣＰコネクション管理部は図１７のステップＳ９２で待っていたＡＣＫであることを識別し、パケット転送用ＴＣＰコネクション管理部１８は通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、これに対応するエントリの通信許可フラグがオン（○）かｏｎｅ－ｗａｙ（△）かを判定し、ｏｎｅ－ｗａｙの場合にはステップＳ１１４に進み、それ以外の場合にはステップＳ１１６に進む。
【０２０２】ステップＳ１１４：既に説明済みの方法に基づいてＡＣＫパケットをルータＢへ転送する。
ステップＳ１１５：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に格納されているエントリを削除する。また、このとき、パケット転送用ＴＣＰコネクション管理部１８は、受信許可ＩＰアドレス保持部１０ａに、エントリの変更後送信元ＩＰアドレスに記載されて

いるダミーアドレスの受信中止を通知し、ダミーＩＰアドレスプール部１５にダミーアドレスを返却する。

【０２０３】ステップＳ１１６：既に説明済みの方法に基づいてＡＣＫパケットをルータＢへ転送する。

ステップＳ１１７：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６に格納されているエントリの通信許可フラグをＯｎｅ－ｗａｙに設定変更する。

【０２０４】以上の処理により、ＴＣＰコネクションを終了することが可能になる。次に、図１９を参照して、ＴＣＰコネクションが切断した場合における復旧処理について説明する。なお、以下では、ルータＡとルータＢの間のコネクションが切断した場合の復旧処理を例に挙げて説明する。

【０２０５】ステップＳ１２０：ルータＡのＴＣＰ部１１がルータＢ間とのＴＣＰコネクションが切断したことを検出する。

【０２０６】ステップＳ１２１：ルータＡのＴＣＰ部１１は、切断したコネクションの両端（ルータＡとルータＢ）それぞれのＩＰアドレスとポート番号をパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０２０７】ステップＳ１２２：ルータＡのパケット転送用ＴＣＰコネクション管理部１８は、ＴＣＰ部１１から受け取ったデータをキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、検索結果のエントリの“通信許可フラグ”をオフにする。

【０２０８】ステップＳ１２３：ルータＡのパケット転送用ＴＣＰコネクション管理部１８は、“送信先端末”フィールドがＮＵＬＬではないことから、ルータＢのポートＸＸとの間で、ＴＣＰコネクションを確立するようにＴＣＰ部１１に指示する。

【０２０９】ステップＳ１２４：既に説明済みの方法に基づいてＮｏｔｉｆｉｃａｔｉｏｎメッセージを送信する。

【０２１０】ステップＳ１２５：既に説明済みの方法に基づいてＡＣＫメッセージを受信する。

ステップＳ１２６：パケット転送用ＴＣＰコネクション管理部１８は、エントリの送信変更後送信元ポートを新しいポート番号(ＶＶ)に書換える。

【０２１１】ステップＳ１２７：パケット転送部１７は、通信許可フラグをオンにする。

ステップＳ１３０：ルータＢのＴＣＰ部がルータＡ間とのＴＣＰコネクション断を検出する。

【０２１２】ステップＳ１３１：ルータＢのＴＣＰ部１１は、切断したコネクションの両端（ルータＡとルータＢ）のそれぞれのＩＰアドレスとポート番号をパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０２１３】ステップＳ１３２：ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、ＴＣＰ部１１から受け取ったデータをキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、検索結果のエントリの“通信許可フラグ”をオフの状態にする。

【０２１４】ステップＳ１３３：ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、“送信先端末”フィールドがＮＵＬＬであることから、ルータＡからのコネクションの再設定を待つ。

【０２１５】ステップＳ１３４：ステップＳ１２４において送信されたＮｏｔｉｆｉｃａｔｉｏｎメッセージを受信する。

【０２１６】ステップＳ１３５：既に説明済みの方法に基づいてＮｏｔｉｆｉｃａｔｉｏｎメッセージに対するＡＣＫメッセージを送信する。

【０２１７】ステップＳ１３６：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の該当するエントリの変更前送信元ポートを新しいポート番号（ＶＶ）に書換える。

【０２１８】ステップＳ１３７：パケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の該当するエントリの通信許可フラグをオンにする。

【０２１９】以上の処理により、ルータＡとルータＢの間のコネクションが切断した場合に、コネクションを復旧することができる。次に、図２０を参照して、ルータＢと端末Ｃとの間のコネクションが切断した場合の復旧処理について説明する。

【０２２０】ステップＳ１４０：ルータＢのＴＣＰ部１１は、端末Ｃとの間のコネクションが切断したことを検出する。

【０２２１】ステップＳ１４１：ルータＢのＴＣＰ部１１は、切断したコネクションの両端（ルータＢと端末Ｃ）のそれぞれのＩＰアドレスとポート番号をパケット転送用ＴＣＰコネクション管理部１８に通知する。

【０２２２】ステップＳ１４２：ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、ＴＣＰ部１１から受け取ったデータをキーとして、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６を検索し、検索結果のエントリの通信許可フラグをオフの状態にする。

【０２２３】ステップＳ１４３：ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、端末Ｃのポート２３番との間で、ＴＣＰコネクションを確立するようにＴＣＰ部１１に指示する。その結果、ＴＣＰコネクションが発呼される。

【０２２４】ステップＳ１４４：ルータＢのパケット転送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の対応するエントリを変更する。即ち、送信元ポートを新しいポート番号（ＵＵ）に書き換える。

【０２２５】ステップＳ１４５：ルータＢのパケット転

送用ＴＣＰコネクション管理部１８は、通信先端末・ゲートウェイＩＰアドレス／ポート保持部１６の対応するエントリの通信許可フラグをオンの状態にする。その結果、端末Ｂとの間でＴＣＰコネクションが確立されることになる。

【０２２６】以上の処理により、ルータＢと端末Ｃとの間のＴＣＰコネクションが切断した場合でも、コネクションを復旧することが可能になる。以上に説明したように、本発明によれば、ユニークなＦＱＤＮ（fully-qualified domain name：ホスト名，ドット，ドメイン名の三つで構成するホストの名前。www.fts.com等）をプライベートアドレス網内の端末に割り当てるようにしたので、プライベートアドレス網、グローバルアドレス網を問わず、ユニークな識別子を端末が有することができる。その結果、プライベートアドレス網同士はそれぞれ重複するアドレス空間を用いているが、プライベートアドレス網内の端末を一意化することが可能になる。

【０２２７】また、本発明によれば、グローバルアドレス網内のＤＮＳサーバのツリーには属さないプライベートアドレス網用のＤＮＳサーバはプライベートアドレス網毎に用意し、これをグローバルアドレス網からアクセスできるようにしたので、グローバルアドレス網経由でプライベートアドレスの名前解決を実現することが可能になる。

【０２２８】更に、本発明によれば、プライベートアドレス網内でのＴＣＰコネクションとグローバルアドレス網内でのＴＣＰコネクションをプライベート網・グローバル網境界ルータ（アドレス変換装置）が別個に張り、ルータが両コネクションをマップ（情報交換）することで、グローバルアドレス網からプライベートアドレス網へのＴＣＰコネクションを実現することが可能になる。

【０２２９】（付記１）　第１のタイプのアドレスを有する通信装置で構成される第１のネットワークに属し、その配下に第２のタイプのアドレスを有する端末で構成される第２のネットワークを有する通信装置において、他の通信装置の配下のネットワークに属する端末に付けられた名前を、当該他の通信装置に付けられた名前と対応して管理する手段と、配下の端末から、通信相手となる端末に付けられた名前を受信した場合、前記管理手段により対応する通信装置に対してアドレス解決の要求を出力する手段と、を設けたことを特徴とする通信装置。

【０２３０】（付記２）　その配下の端末のアドレスをその端末に付けられた名前と対応させて管理する手段と、前記他の通信装置からのその配下の端末のアドレス解決の要求に対して、前記管理手段によりアドレスを解決して、前記他の通信装置へ解決したアドレスを通知する手段と、を設けたことを特徴とする付記１記載の通信装置。

【０２３１】（付記３）　アドレス解決の要求に対してアドレスの解決通知を前記他の通信装置から受信した場合、通知を受けたアドレスを前記第２のタイプのアドレスであって、その配下のネットワークの端末のアドレスとして用いられないアドレスに変換したダミーアドレスと対応づけて管理する手段と、変換後の前記アドレスを通信を要求した端末へ通知する手段と、を設けたことを特徴とする付記２記載の通信装置。

【０２３２】（付記４）　通信を要求した端末から、通知後のダミーアドレスを持つパケットを受信した場合、ダミーアドレスを前記他の通信装置のアドレスに変換する手段を設けたことを特徴とする付記３記載の通信装置。

【０２３３】（付記５）　第１のタイプのアドレスを有する通信装置で構成される第１のネットワークと、通信装置の配下で第２のタイプのアドレスを有する端末で構成される第２のネットワークとからなるネットワークシステムにおいて、前記通信装置には、その配下の端末のアドレスをそれぞれの端末に付けられた名前と対応させて管理する第１の管理手段と、端末の名前をその端末のアドレスを管理する通信装置と対応させて管理する第２の管理手段と、を設け、配下の端末からの通信要求に対して通信相手の端末のアドレスを解決する他の通信装置を前記第２の管理手段により求め、他の通信装置で前記第１の管理手段によりアドレス解決を行うことを特徴とするネットワークシステム。

【０２３４】（付記６）　各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、これらの間でデータを伝送する際にアドレスの変換を行なうアドレス変換装置とを有するネットワークシステムにおいて、前記アドレス変換装置は、前記プライベートアドレス網に属する各ノードに対して、ユニークな名前を付与して管理し、前記グローバルアドレス網または他のプライベートアドレス網に属する所定のノードから所定の名前に対する問い合わせがなされた場合には、対応するプライベートアドレスを取得して通知する、ことを特徴とするネットワークシステム。

【０２３５】（付記７）　送信端末側に配置された他のアドレス変換装置を更に有し、前記他のアドレス変換装置には、各ノードに付与されているユニークな名前が予め登録されていることを特徴とする付記６記載のネットワークシステム。

【０２３６】（付記８）　各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、前記グローバルアドレス網におけるアドレス変換を行なう第１のアドレス変換装置と、前記グローバルアドレス網と前記プライベートアドレス網との間におけるアドレス変換を行なう第２のアドレス変換装置とを有するネットワークシステムにおいて、前記第１および第２のアドレス変換装置は、それぞれ独立にコネクションを確立し、相互にコ

ネクションに関する情報を交換することにより、前記グローバルアドレス網と、前記プライベートネットワーク網との間で、データの授受を可能とする、ことを特徴とするネットワークシステム。

【０２３７】（付記９）　前記第１のアドレス変換装置は、送信端末がコネクションを確立する際に、前記コネクションに関する情報を前記第２のアドレス変換装置に通知することを特徴とする付記８記載のネットワークシステム。

【０２３８】（付記１０）　前記第１のアドレス変換装置は、受信端末の実際のプライベートアドレスとは異なるダミーのアドレスを前記送信端末に対して通知することを特徴とする付記９記載のネットワークシステム。

【０２３９】（付記１１）　前記ダミーのアドレスは、前記受信端末の実際のプライベートアドレスとはネットワーククラスが異なるアドレスであることを特徴とする付記１０記載のネットワークシステム。

【０２４０】（付記１２）　前記第２のアドレス変換装置は、前記受信端末との間のコネクションが切断された場合には、前記第１のアドレス変換装置から通知された前記コネクションに関する情報を参照して、コネクションを再度確立し直すことを特徴とする付記９記載のネットワークシステム。

【０２４１】（付記１３）　前記第１のアドレス変換装置は、前記第２のアドレス変換装置との間のコネクションが切断された場合には、受信端末に関する情報を参照し、前記第２のアドレス変換装置との間に新たにコネクション確立するとともに、前記第２のアドレス変換装置に前記コネクションに関する情報を通知し、前記第２のアドレス変換装置は、前記第１のアドレス変換装置から通知された前記コネクションに関する情報に基づいてコネクションを更新する、ことを特徴とする付記９記載のネットワークシステム。

【０２４２】（付記１４）　前記第１および第２のアドレス変換装置は、コネクションの状態を示す情報を保持し、この情報に基づいてデータを転送することを特徴とする付記９記載のネットワークシステム。

【０２４３】（付記１５）　前記コネクションの状態を示す情報は、コネクションの確立中、片方向のみ確立済み、または、通信可能のいずれかを示す情報であることを特徴とする付記９記載のネットワークシステム。

【０２４４】（付記１６）　各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網との間でデータを伝送する際にアドレスの変換を行なうアドレス変換装置において、前記プライベートアドレス網に属する各ノードに対して、ユニークな名前を付与して管理し、前記グローバルアドレス網または他のプライベートアドレス網に属する所定のノードから所定の名前に対する問い合わせがなされた場合には、対応するプライベートアドレスを取得して通知する、ことを特徴とするアドレス変換装置。

【０２４５】（付記１７）　各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、前記グローバルアドレス網と前記プライベートアドレス網との間におけるアドレス変換を行なう他のアドレス変換装置とを有するネットワークに接続され、前記グローバルアドレス網におけるアドレス変換を行なうアドレス変換装置において、前記他のアドレス変換装置とは独立にコネクションを確立し、前記他のアドレス変換装置との間で相互にコネクションに関する情報を交換することにより、前記グローバルアドレス網と、前記プライベートネットワーク網との間で、データの授受を可能とすることを特徴とするアドレス変換装置。

【０２４６】（付記１８）　前記アドレス変換装置は、送信端末がコネクションを確立する際に、前記コネクションに関する情報を前記他のアドレス変換装置に通知することを特徴とする付記１７記載のアドレス変換装置。

【０２４７】（付記１９）　前記アドレス変換装置は、受信端末の実際のプライベートアドレスとは異なるダミーのアドレスを送信端末に対して通知することを特徴とする付記１８記載のアドレス変換装置。

【０２４８】（付記２０）　前記ダミーのアドレスは、前記受信端末の実際のプライベートアドレスとはネットワーククラスが異なるアドレスであることを特徴とする付記１９記載のアドレス変換装置。

【０２４９】

【発明の効果】以上説明したように本発明では、第１のタイプのアドレスを有する通信装置で構成される第１のネットワークに属し、その配下に第２のタイプのアドレスを有する端末で構成される第２のネットワークを有する通信装置において、他の通信装置の配下のネットワークに属する端末に付けられた名前を、当該他の通信装置に付けられた名前と対応して管理する手段と、配下の端末から、通信相手となる端末に付けられた名前を受信した場合、管理手段により対応する通信装置に対してアドレス解決の要求を出力する手段と、を設けるようにしたので、プライベートアドレス網、グローバルアドレス網を問わず、ユニークな識別子を端末に付与することができる。

【０２５０】また、以上説明したように本発明では、第１のタイプのアドレスを有する通信装置で構成される第１のネットワークと、通信装置の配下で第２のタイプのアドレスを有する端末で構成される第２のネットワークとからなるネットワークシステムにおいて、通信装置には、その配下の端末のアドレスをそれぞれの端末に付けられた名前と対応させて管理する第１の管理手段と、端末の名前をその端末のアドレスを管理する通信装置と対応させて管理する第２の管理手段と、を設け、配下の端

末からの通信要求に対して通信相手の端末のアドレスを解決する他の通信装置を第２の管理手段により求め、他の通信装置で第１の管理手段によりアドレス解決を行うようにしたので、ユニークな識別子を端末に付与し、その識別しに基づいて通信を行うことが可能になる。

【０２５１】また、以上説明したように本発明では、各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、これらの間でデータを伝送する際にアドレスの変換を行なうアドレス変換装置とを有するネットワークシステムにおいて、アドレス変換装置は、プライベートアドレス網に属する各ノードに対して、ユニークな名前を付与して管理し、グローバルアドレス網または他のプライベートアドレス網に属する所定のノードから所定の名前に対する問い合わせがなされた場合には、対応するプライベートアドレスを取得して通知するようにしたので、プライベートアドレス網またはグローバルアドレス網の別を問わず、ユニークな識別子を各ノードが有することが可能になる。

【０２５２】更に、本発明では、各ノードがユニークなアドレスを有するグローバルアドレス網と、ユニークでないアドレスを有するプライベートアドレス網と、グローバルアドレス網におけるアドレス変換を行なう第１のアドレス変換装置と、グローバルアドレス網とプライベートアドレス網との間におけるアドレス変換を行なう第２のアドレス変換装置とを有するネットワークシステムにおいて、第１および第２のアドレス変換装置は、それぞれ独立にコネクションを確立し、相互にコネクションに関する情報を交換することにより、グローバルアドレス網と、プライベートネットワーク網との間で、データの授受を可能とするようにしたので、グローバルアドレス網からプライベートアドレス網へのコネクションを確立することが可能になる。

【図面の簡単な説明】

【図１】本発明の実施の形態の構成を示す図である。

【図２】ルータの詳細な構成例を示す図である。

【図３】プライベート網に属する端末Ａが同じくプライベート網に属する端末Ｂに対してアクセスする際の名前解決処理について説明するシグナルフロー図である。

【図４】通信先プライベート網用名前解決サーバ登録部に登録されている情報のフォーマットを説明する図である。

【図５】ＴＣＰコネクションを確立する場合の処理について説明するシグナルフロー図である。

【図６】ＴＣＰコネクションを確立する場合の処理について説明するシグナルフロー図である。

【図７】通信先端末・ゲートウェイＩＰアドレス／ポート保持部に登録されているエントリのフォーマットを説明する図である。

【図８】ＴＣＰコネクションを利用してパケットを転送する場合の処理について説明するシグナルフロー図である。

【図９】ＴＣＰコネクションを終了する際に、双方向の通信を片方向に変更する場合の処理について説明するシグナルフロー図である。

【図１０】ＴＣＰコネクションを終了する際に、片方向の通信を終了する場合の処理について説明するシグナルフロー図である。

【図１１】ルータＡとルータＢとの間のコネクションが切断した場合において、これを復旧する際の処理について説明するシグナルフロー図である。

【図１２】ルータＢと端末Ｃとの間のコネクションが切断した場合において、これを復旧する際の処理について説明するシグナルフロー図である。

【図１３】名前解決処理が実行される際のルータＡにおける処理の流れを説明するフローチャートである。

【図１４】ＴＣＰコネクションを確立する際の処理について説明するフローチャートである。

【図１５】ＴＣＰコネクションを確立する際の処理について説明するフローチャートである。

【図１６】図１４および図１５の処理によって確立されたＴＣＰコネクションを利用してパケットを転送する際の処理について説明するフローチャートである。

【図１７】ＴＣＰコネクションを終了する際にルータＡおよびルータＢにおいて実行される処理について説明するフローチャートである。

【図１８】ＴＣＰコネクションを終了する際にルータＡおよびルータＢにおいて実行される処理について説明するフローチャートである。

【図１９】ＴＣＰコネクションが切断した場合における復旧処理について説明するフローチャートである。

【図２０】ルータＢと端末Ｃとの間のコネクションが切断した場合の復旧処理について説明するフローチャートである。

【図２１】各クラスのＩＰアドレスの構成を示す図である。

【図２２】各クラスのＩＰアドレスに使用される数字の範囲を説明するための図である。

【図２３】ＲＦＣ１５９７に規定されているプライベートＩＰアドレスの数値を示す図である。

【図２４】公報中に記載されている図１に記載されているインターネットワーク環境のブロック図に同公報の説明内容を要約して付加して示した図である。

【図２５】ＮＡＴ機能を説明する図である。

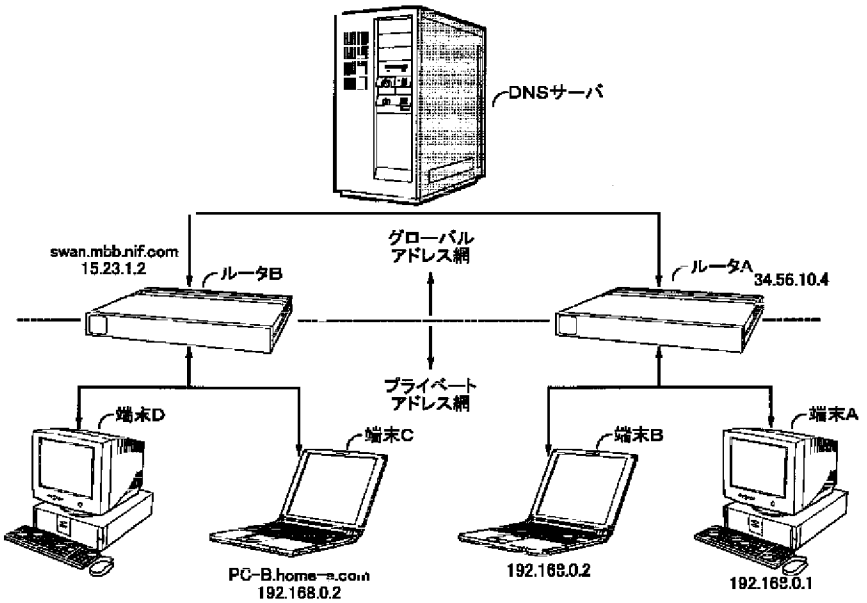
【図２６】ＩＰマスカレードにおけるネットワークの構成とＩＰアドレスの使用形態のモデルを示す図である。

【図２７】ＩＰマスカレードにおけるプライベートＩＰアドレスとグローバルＩＰアドレスの対応の一例を示す図である。

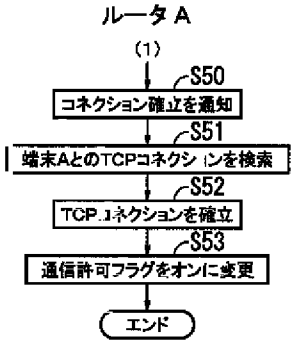
【符号の説明】

１０　ＩＰ部
１０ａ　受信許可ＩＰアドレス保持部
１１　ＴＣＰ部
１１ａ　受信ポート変更部
１２　名前解決部
１３　プライベート網宛名前解決判定部
１４　通信先プライベート網用名前解決サーバ登録部
１５　ダミーＩＰアドレスプール部
１６　通信先端末・ゲートウェイＩＰアドレス／ポート保持部
１７　パケット転送部
１８　パケット転送用ＴＣＰコネクション管理部
１９　通信先端末アドレス／ポートネゴシエーション部
２０　通信手段
２１　コンソール

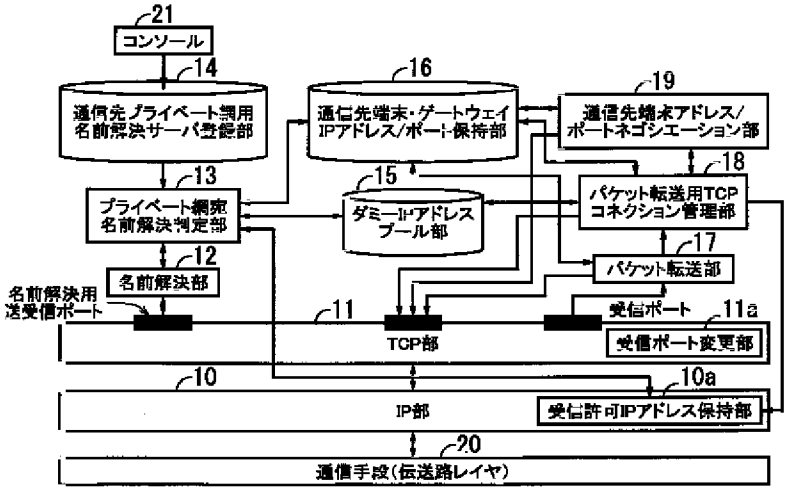
【図１】



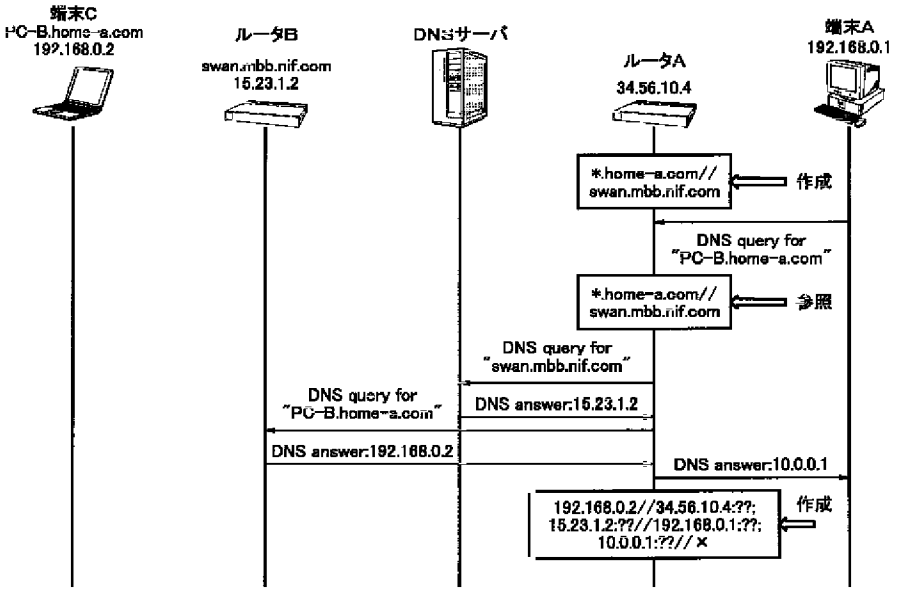
【図１５】



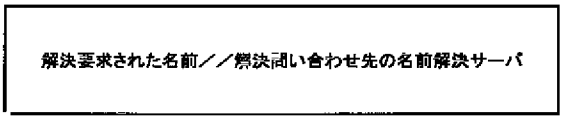
【図２】



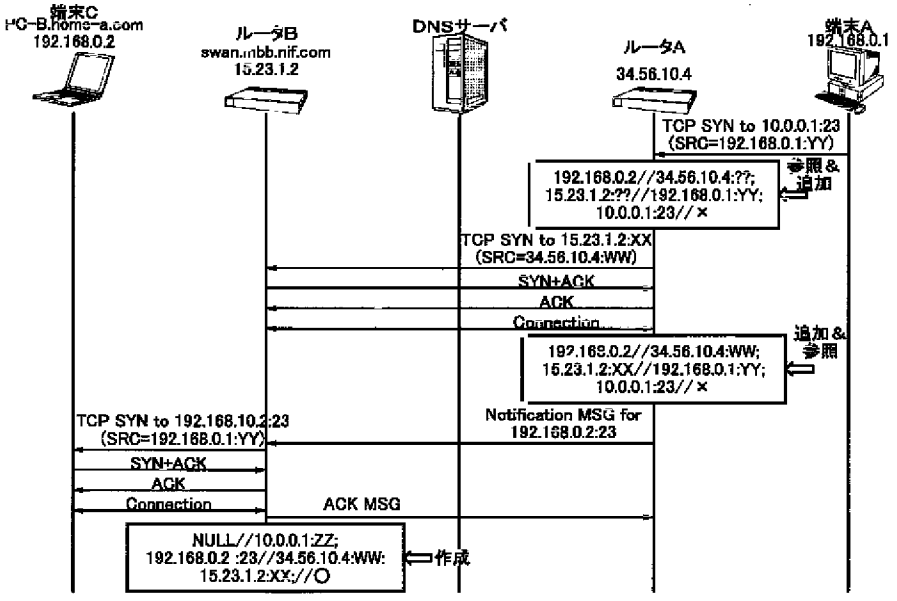
【図3】


端末C
PC-B.home-a.com
192.168.0.2
ルータB
swan.mbb.nif.com
15.23.1.2
DNSサーバ
ルータA
34.56.10.4
端末A
192.168.0.1
*.home-a.com//
swan.mbb.nif.com
作成
DNS query for
"PC-B.home-a.com"
*.home-a.com//
swan.mbb.nif.com
参照
DNS query for
"swan.mbb.nif.com"
DNS query for
"PC-B.home-a.com"
DNS answer:15.23.1.2
DNS answer:192.168.0.2
DNS answer:10.0.0.1
192.168.0.2//34.56.10.4:??;
15.23.1.2:??//192.168.0.1:??;
10.0.0.1:??//×
作成

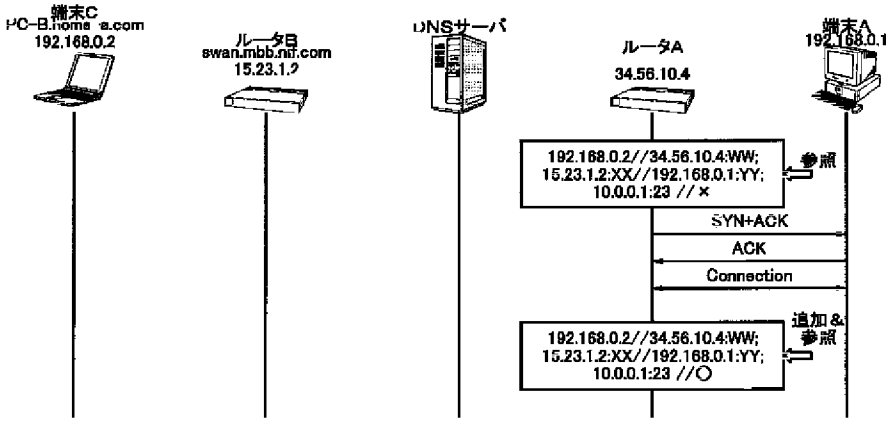
【図4】


解決要求された名前／／解決問い合わせ先の名前解決サーバ

【図5】


端末C
PC-B.home-a.com
192.168.0.2
ルータB
swan.mbb.nif.com
15.23.1.2
DNSサーバ
ルータA
34.56.10.4
端末A
192.168.0.1
TCP SYN to 10.0.0.1:23
(SRC=192.168.0.1:YY)
192.168.0.2//34.56.10.4:??;
15.23.1.2:??//192.168.0.1:YY;
10.0.0.1:23//×
参照&
追加
TCP SYN to 15.23.1.2:XX
(SRC=34.56.10.4:WW)
SYN+ACK
ACK
Connection
192.168.0.2//34.56.10.4:WW;
15.23.1.2:XX//192.168.0.1:YY;
10.0.0.1:23//×
追加&
参照
TCP SYN to 192.168.10.2:23
(SRC=192.168.0.1:YY)
Notification MSG for
192.168.0.2:23
SYN+ACK
ACK
Connection
ACK MSG
NULL//10.0.0.1:ZZ;
192.168.0.2 :23//34.56.10.4:WW;
15.23.1.2:XX;//○
作成

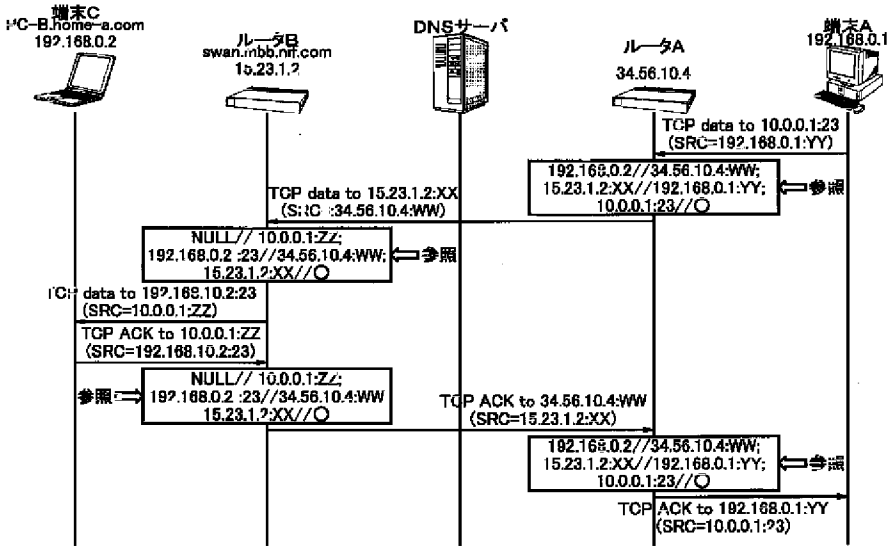
【図6】



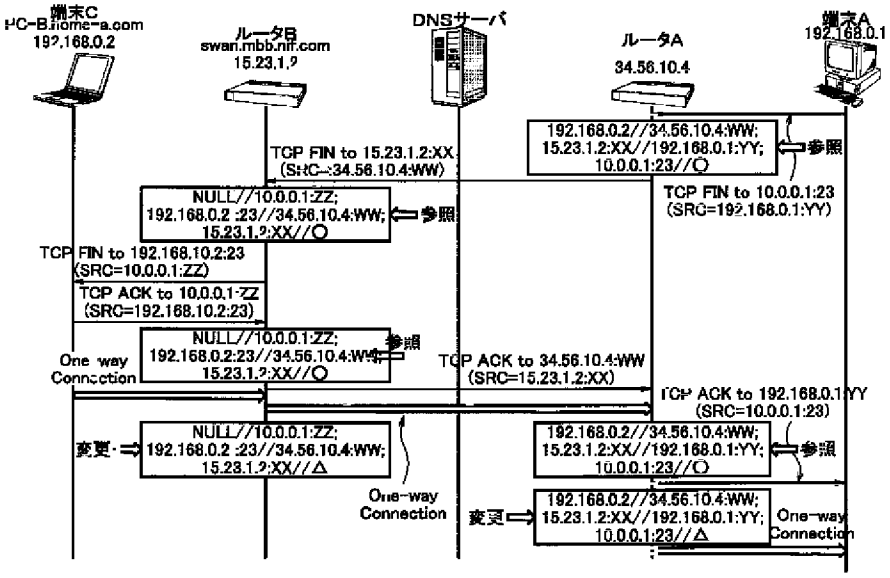
【図7】

受信端末(インターネット上のTCPのコネクションを確立する側のルータのみ保持)／／
変更後送信元IPアドレス:変更後送信元ポート;変更後送信先IPアドレス:変更後送信先ポート／／
変更前送信元IPアドレス:変更前送信元ポート;変更前送信先IPアドレス:変更前送信先ポート／／
通信許可フラグ

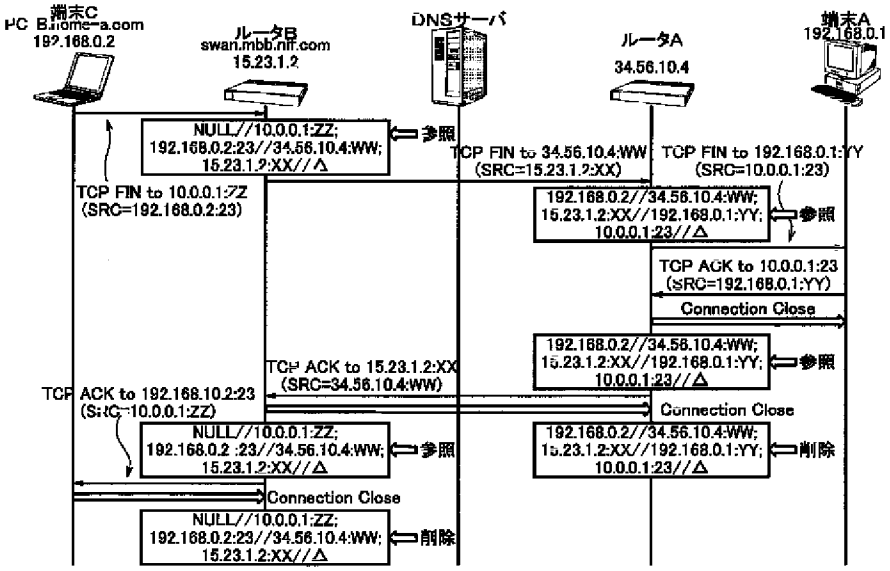
【図8】



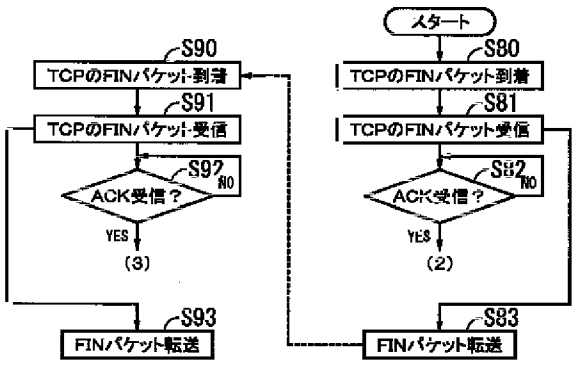
【図９】



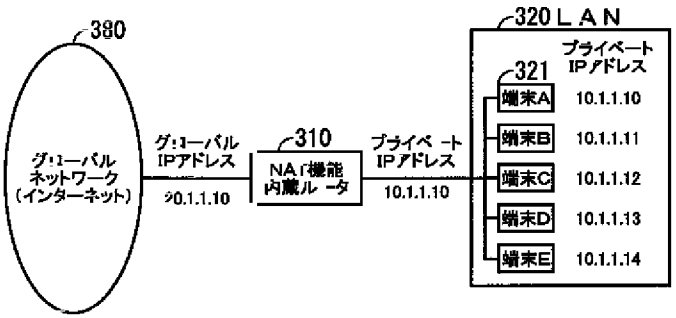
【図１０】



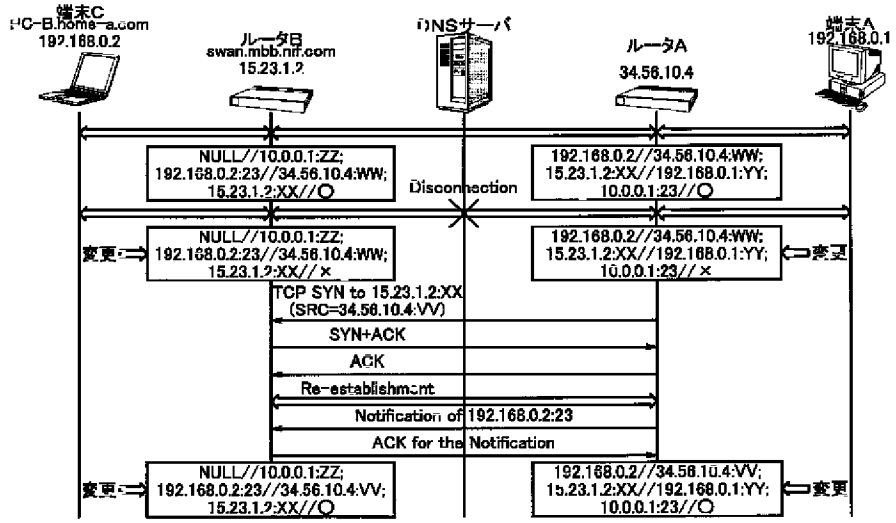
【図１７】



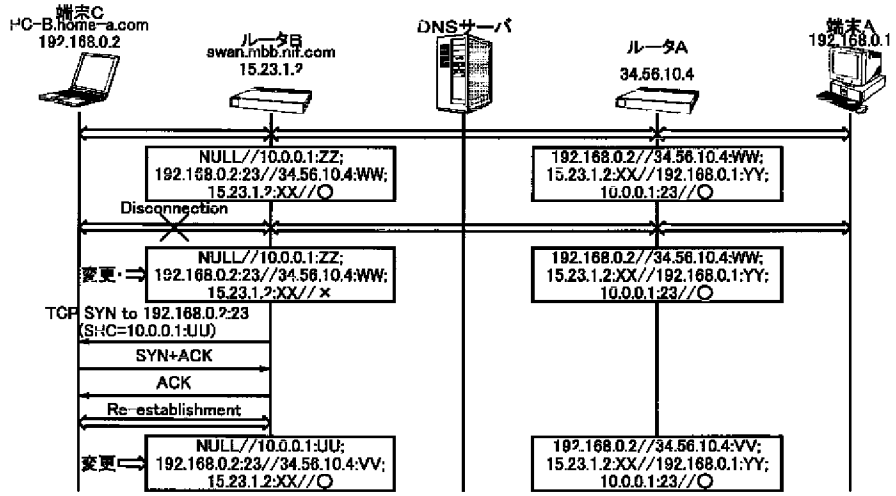
【図２５】



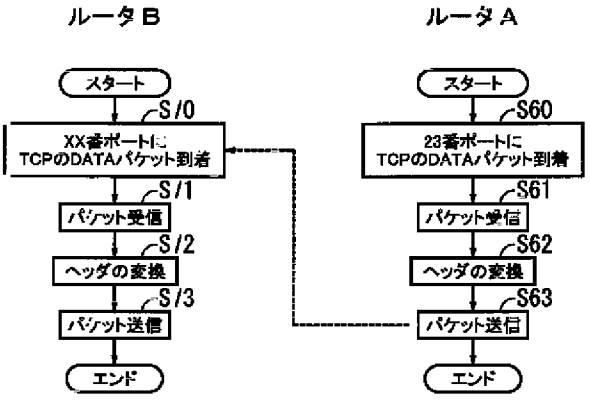
【図１１】



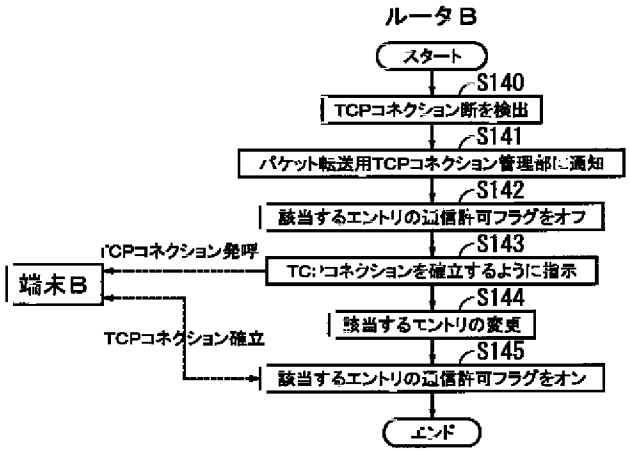
【図１２】



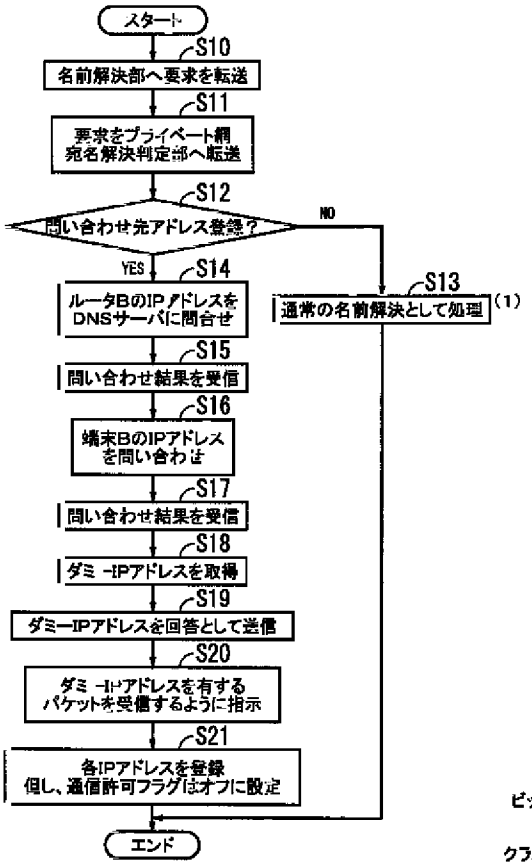
【図１６】



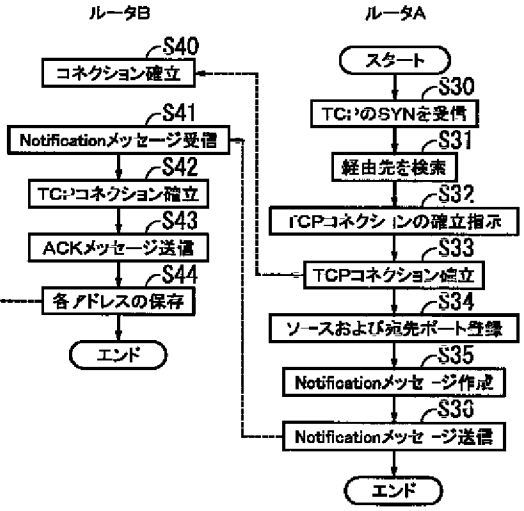
【図２０】



【図１３】



【図１４】

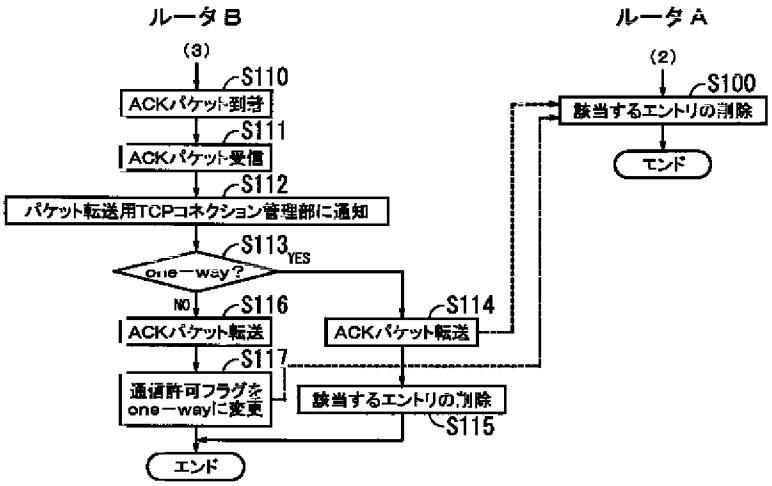


【図２２】

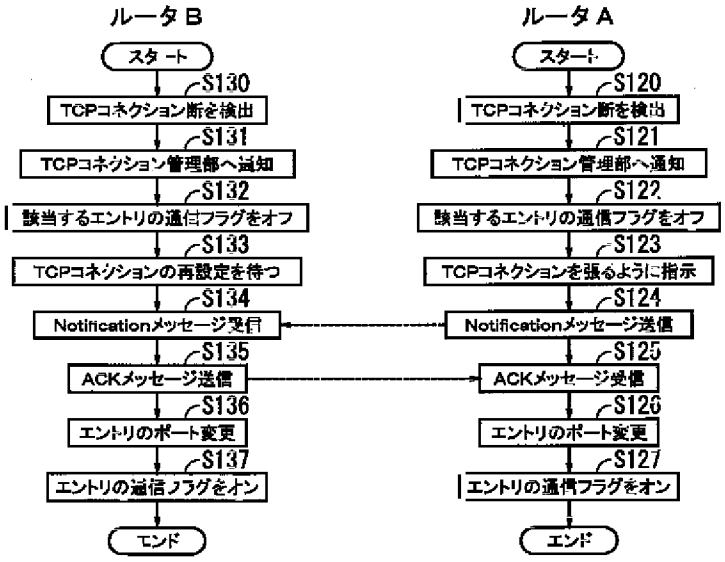
一般構成(クラスA～C)

ビット	0 7	13	27	31	IPアドレスの表現方法
クラスA	0～127	S/H(0～255)	S/H(0～255)	H(0～255)	10. H. H. H
クラスB	128～191	0～255	S/H(0～255)	H(0～255)	128. 20. H. H
クラスC	192～223	0～255	0～255	H(0～255)	192. 30. 100. H

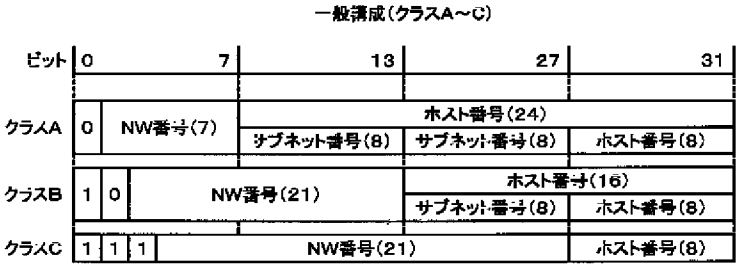
【図１８】



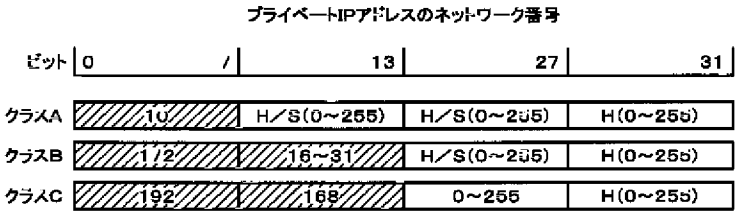
【図１９】



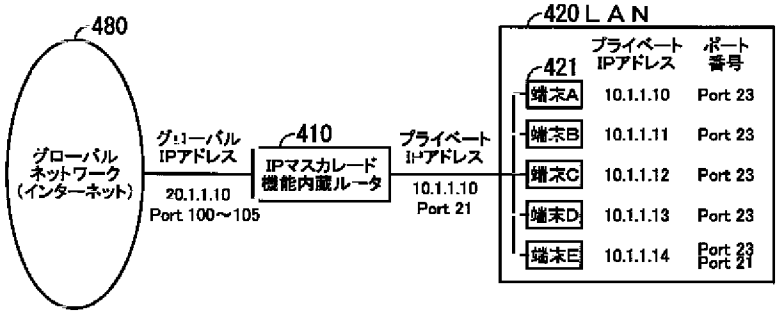
【図２１】



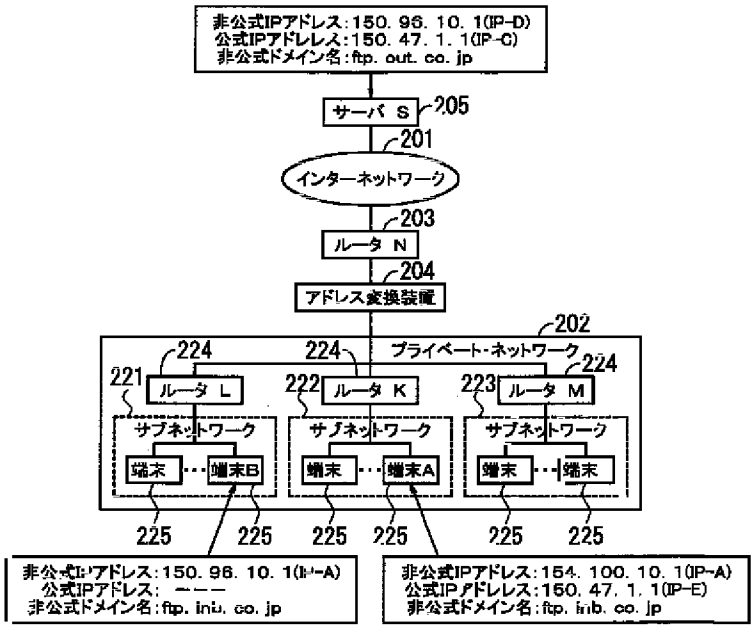
【図２３】



【図２６】



【図２４】



【図２７】

アプリケーション	グローバル・ネットワーク側（インターネット側）		プライベート・ネットワーク側（端末側）	
	IPアドレス	ポート番号	IPアドレス	ポート番号
Telnet	20.1.1.10	100	10.1.1.10	23
Telnet	20.1.1.10	101	10.1.1.11	23
Telnet	20.1.1.10	102	10.1.1.12	23
Telnet	20.1.1.10	103	10.1.1.13	23
Telnet	20.1.1.10	104	10.1.1.14	23
FTP	20.1.1.10	105	10.1.1.14	21